


3 1761 11649423 8



Digitized by the Internet Archive
in 2023 with funding from
University of Toronto

<https://archive.org/details/31761116494238>



CA1
Z 4
-C 52

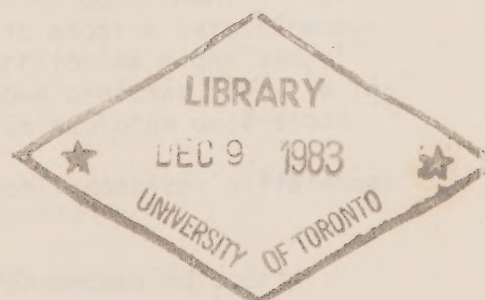
DOCUMENT: 870-112/029

Government
Publications

MEETING OF THE INTERPROVINCIAL
SPORT AND RECREATION COUNCIL

Report of the Committee on Sport Recognition

Federal



Ottawa, Ontario
April 20, 1983

April 1983

ISRC

REPORT OF THE COMMITTEE ON SPORT RECOGNITION

ISSUE: The feasibility of developing and adopting a common definition of sport and criteria for recognition of sport organizations.

BACKGROUND: The ISRC Committee (including federal representation) was established at the June 1982 ISRC meeting. Since that time the Committee has met on four occasions and circulated questionnaires/documents to provinces-territories on two occasions. An initial report was distributed to ISRC members for reaction in the Fall of 1982 and the Committee met in March 1983 to prepare its final report.

ALTERNATIVES: The original questionnaire and subsequent report to which ISRC members responded indicated that consensus would be difficult to achieve. It was clearly not feasible to propose adoption of a common definition and common criteria for recognition of sport organizations. There was greater consensus on the matter of the definition of sport than there was on the issue of recognition criteria. Similarly, there was consensus on the matter of each level of government having the right to set its own criteria, and for these criteria to be accepted by other levels of government - i.e. if the federal government chose to adopt a set of recognition criteria, provinces-territories might adopt different criteria for their own purposes, but the integrity of the federal criteria would be understood.

There were a couple of clear philosophical differences on this general subject area:

(1) definition of recreation encompassing sport

(2) the rather broad definition of a sport organization in vogue among some provinces and the federal government - i.e. the concept of a sport governing body expanded beyond its traditional role as a governing body to a role as a service agency.

ALTERNATIVES: The following two alternatives were considered by the Committee:

- A. Try again to obtain consensus among the provinces-territories and federal governments by means of another questionnaire.
- B. Utilize the work undertaken by the Recognition Committee to date, and encourage each government to use the information as it sees fit.

RECOMMENDATION:

- (1) That the federal government and each province-territory should have a written and well-publicized definition of sport.
- (2) That the federal government and provinces-territories should use the definition and criteria for recognition developed by the Committee.
- (3) That continued dialogue and information sharing on sport recognition take place on an ad hoc basis.

IMPLICATIONS:

- (1) In view of the fact that the Committee could not identify clear consensus, there is a danger that continued unilateral action on the part of each government may cause some confusion and lead to pressure being exerted on jurisdictions which have adopted stricter criteria than other jurisdictions.
- (2) Providing that each level of government accepts the integrity of the criteria of other governments, there should be no financial implications.

(See Appendix for details)

REPORT OF THE COMMITTEE ON SPORT RECOGNITION

APPENDIX:

A. DEFINITION OF SPORT:

SPORT is a physical activity which involves the use of large muscle groups, requires mental preparation and strategic methods and whose outcome is determined by skill not chance. It is an activity traditionally regarded as a sport, for which the participants have practised or trained extensively, utilizing the application of scientific knowledge usually under the direction of a coach. It is governed by a standard set of rules and occurs in an organized, structured environment in which a winner is declared and the outcome is determined primarily by human physical actions.

B. DEFINITION OF A SPORT GOVERNING BODY:

A SPORT GOVERNING BODY is a non-profit voluntary organization which provides leadership in technical, educational and administrative service areas to its members and to practitioners of a sport who may or may not be members but who participate on an organized basis.

Among the objectives of sport governing bodies are: advancing the enjoyment of all participants and supporting the excellence aspirations of high performance athletes.

C. CRITERIA FOR RECOGNITION:

Several provinces-territories have written criteria for the recognition of sport governing bodies. The Committee recommends the adoption of criteria using the following framework. Specific standards and performance levels should be set by each government - the following information simply identifies the subject areas within which more specific criteria should be defined:

- Governing/Organizational Structure
- Membership
- Financial Status
- Administration
- Programs

CRITERIA FOR RECOGNITION:

1. Governing/Organizational Structure -

A recognized sport organization has a definable, visible leadership, planning and decision-making structure.

Possible Factors:

- reliance on voluntary effort
- elections
- AGM
- Board/Executive/regional representation
- circulation of minutes of meetings
- democratic decision-making structures
- constitution/by-laws
- registered under the Societies Act (federal/provincial)

2. Membership -

A recognized sport organization has a minimum number of competitors and sufficient participation in various roles and at various levels.

Possible Factors:

- registered membership base of 'x' number of competitors, participants in competitive or non-competitive programs
- numbers of athletes, coaches, officials, volunteer administrators
- geographic distribution of members/participants
- communication with membership

3. Financial Status -

A recognized sport organization has the ability both to generate and to properly manage funds.

Possible Factors:

- audited financial statement
- fund-raising capacity
- non-profit status

APPENDIX (3)

4. Administration -

A recognized sport organization has the capacity to plan, implement and evaluate its activities on an on-going basis and in accordance with known association management practices.

Possible Factors:

- delivery of technical, educational and administrative services to members and the public
- capacity to promote, develop and govern the sport
- logical affiliation network from local to national levels
- provision of regular information to membership through newsletters, publications etc.

5. Programs -

A recognized sport organization provides a range of competition, leadership training, technical development and promotion programs for its members and prospective participants.

Possible Factors -

- competitions (including championships)
- leadership training - coaches
 - officials
 - administrators
 - volunteers and professionals
- athlete development programs
- promotion/information programs

APPENDIX (4)

E. ISRC INPUT

ISRC members were asked on two occasions to provide input to the Committee on Sport Recognition.

The responses to the first questionnaire are contained on the attached sheet dated October 1982.

ISRC members were again asked to respond to the initial report of the Recognition Committee (report dated 20.09.82 - draft 1). Five responses were received.

Appendix 'A'

FEDERAL-PROVINCIAL COMMITTEEON SPORT RECOGNITIONQuestionnaire - Summary Results

- # 1. Does your province/territory have a written policy outlining conditions for a sport to be recognized by government ? YES - 9 NO - 2
- # 2. Does your province/territory have a written policy outlining what characteristics or qualities an activity must have in order to be defined as a sport? YES - 6 NO - 5
- # 3. What level of support from a provincial/terr. government should be provided in order for the federal government to consider that the sport is "recognized" in a particular province ? NO CLEAR CONSENSUS.
Many respondents indicated that if the provincial/terr. govt. recognized the sport, then that should be the main criteria. There was general opposition to simple and crude measures such as the amount of provincial financial support.
- # 4. Do you think it would be advisable to establish common criteria for all provinces and territories as a minimum condition for recognition by government ? YES - 7 NO - 4
- # 5. Would your province/terr. be agreeable if minimum conditions for considering a sport to be recognized within a prov./terr. were established by the federal govt. for the purpose of determining which sports the federal government should recognize? YES - 6 NO - 5
(Responses unclear - some favoured general agreement among provs. on criteria, while others concede federal 'right' to determine own

CA1
Z 4
-C 52

DOCUMENT: 870-112/029

Traduction du Secrétariat

REUNION DU CONSEIL INTERPROVINCIAL
DU SPORT ET DES LOISIRS

Rapport du comité de reconnaissance des diciplines sportives

Fédéral



Ottawa (Ontario)
Le 20 avril 1983

CISL

RAPPORT DU COMITE DE RECONNAISSANCE DES DISCIPLINES SPORTIVES

QUESTION A L'ETUDE: La possibilité d'établir et d'adopter une définition commune des disciplines sportives et des critères de reconnaissance des associations sportives.

HISTORIQUE: La comité du CISL (y compris les représentants fédéraux) a été mis sur pied au cours de la réunion du Conseil de juin 1982. Dupuis, le comité s'est réuni à quatre occasions et a diffusé deux fois des questionnaires et des documents aux provinces et aux territoires. A l'automne de 1982 a été communiqué aux membres un premier rapport dans lequel on leur demandait de faire connaître leurs réactions, et le comité s'est réuni en mars 1983 afin de préparer son rapport final.

SOLUTIONS POSSIBLES: Les réponses apportées par les membres au questionnaire initial et leurs réactions au rapport publié par la suite ont démontré qu'il serait difficile de faire l'unanimité. Il était évident qu'il serait impossible de proposer l'adoption d'une définition et de critères communs de reconnaissance des associations sportives. La question de la définition des disciplines sportives a davantage rallié les opinions que celle des critères de reconnaissance. De même, on s'est entendu pour dire que chaque palier de gouvernement doit avoir le droit d'établir ses propres critères et que ces critères doivent être acceptés par les autres paliers, c'est-à-dire que si le gouvernement fédéral choisit d'adopter certains critères de reconnaissance, les provinces et les territoires peuvent en adopter d'autres pour leurs propres besoins, mais ils doivent reconnaître l'intégrité des critères fédéraux.

Deux philosophies différentes se dégagent de ce sujet global, à savoir :

- (1) La définition des loisirs englobant les sport
- (2) La définition plutôt vaste d'une association sportive qui a cours actuellement dans certaines provinces et au gouvernement fédéral, c'est-à-dire le principe voulant que le rôle traditionnel d'organisme de régie d'une fédération sportive s'étende à un rôle d'organisme de service.

SOLUTIONS POSSIBLES: Le comité a étudié les deux solutions suivantes :

- A. Tenter de nouveau d'obtenir un consensus entre les gouvernements provinciaux, territoriaux et fédéral par le biais d'un autre questionnaire.
- B. Utiliser les travaux effectués jusqu'ici par le comité de reconnaissance et encourager chaque gouvernement à se servir des renseignements comme bon lui semble.

RECOMMANDATION :

- (1) Que le gouvernement fédéral et chaque province ou territoire rédige et fasse connaître sa propre définition des disciplines sportives.
- (2) Que le gouvernement fédéral et les provinces ou territoires devraient utiliser la définition et les critères de reconnaissance établis par le comité.
- (3) Que le dialogue et l'échange de renseignements sur la reconnaissance des disciplines sportives se poursuivent au besoin.

REPERCUSSIONS :

- (1) Comme le comité n'a pas pu dégager un consensus net, il se peut qu'il y ait une certaine confusion si chaque gouvernement continue d'agir unilatéralement et que des pressions soient exercées auprès des administrations qui ont adopté des critères plus sévères que les autres.
- (2) Pourvu que chaque palier de gouvernement reconnaisse l'intégrité des critères des autres paliers, il ne devrait y avoir aucune répercussion financière.

(Voir les détails à l'annexe)

RAPPORT DU COMITE DE RECONNAISSANCE DES DISCIPLINES SPORTIVES

ANNEXE:

A. DEFINITION DU SPORT:

Un SPORT est une activité physique qui fait intervenir un groupe important de muscles, qui exige une préparation mentale et des méthodes stratégiques, et dont le résultat est déterminé par l'adresse et non par la chance. C'est une activité qui a toujours été considérée comme un sport, qui demande de l'exercice ou un entraînement intensif, et qui fait appel à l'application de connaissances scientifiques habituellement sous la direction d'un entraîneur. Un sport est régi par des règles reconnues et se déroule dans un milieu organisé et structuré qui détermine un gagnant et dont l'issue découle principalement d'une activité physique humaine.

B. DEFINITION D'UNE FEDERATION SPORTIVE:

Une FEDERATION SPORTIVE est un organisme bénévole à but non lucratif qui dispense des services d'animation, d'éducation et d'administration ainsi que des services techniques à ses membres et aux adeptes de ce sport qui ne sont peut-être pas membres de l'organisme mais qui participent à une certaine variante organisée de la discipline en question.

Les objectifs des fédérations sportives comprennent entre autres : améliorer le plaisir de tous les participants et appuyer les aspirations d'excellence des athlètes de haut calibre.

C. CRITERES DE RECONNAISSANCE:

Plusieurs provinces et territoires ont établi par écrit des critères de reconnaissance des fédérations sportives. Le Comité recommande l'adoption de critères selon le cadre proposé ci-après. Les normes et les niveaux de performance particuliers relèvent de chaque gouvernement et les renseignements qui suivent ne font que répertorier les domaines que chaque province ou territoire peut adapter à ses propres besoins :

- Structure de régie et d'organisation
- Mode d'adhésion
- Situation financière
- Administration
- Programmes

CRITERES DE RECONNAISSANCE :

1. Structure de régie et d'organisation -

Une association sportive reconnue doit avoir une structure d'animation, de planification et de prise de décision établie et visible.

Facteurs éventuels :

- bénévolat
- élections
- assemblée générale annuelle
- conseil d'administration, comité exécutif et représentation régionale
- diffusion du procès-verbal des réunions
- structures décisionnelles démocratiques
- constitution et règlements
- enregistrement en vertu d'une loi sur les sociétés (fédérale ou provinciale)

2. Mode d'adhésion -

Une association sportive reconnue a un nombre minimal de compétiteurs et elle a suffisamment de participants jouant des rôles divers à différents paliers.

Facteurs éventuels :

- nombre x de membres inscrits au niveau des compétiteurs et des participants à des programmes comportant ou non compétition
- un certain nombre d'athlètes, d'entraîneurs, d'officiels, d'administrateurs bénévoles
- répartition des membres et des participants par secteur géographique
- communication avec les membres

3. Situation financière -

Une association sportive reconnue est en mesure de recueillir et de gérer sainement des sommes d'argent.

Facteurs éventuels :

- vérification de l'état financier
- capacité de recueillir des sommes d'argent
- organisme à but non lucratif

4. Administration -

Une association sportive reconnue peut planifier, mettre en oeuvre et évaluer ses activités de façon permanente et conformément aux pratiques reconnues de gestion des associations.

Facteurs éventuels :

- présentation de services techniques et de services d'éducation et d'administration aux membres et au grand public
- capacité de promouvoir, de mettre en valeur et de régir une discipline sportive
- réseau logique d'affiliation du niveau local au niveau national
- diffusion régulière de renseignements aux membres par l'entremise de bulletins, de publications, etc.

5. Programmes -

Une association sportive reconnue assure toute une gamme de programmes de compétition, de formation en animation, de perfectionnement technique et de mise en valeur pour ses membres et les participants éventuels.

Facteurs éventuels :

- compétitions (y compris des championnats)
- formation en animation
 - entraîneurs
 - officiels
 - administrateurs
 - bénévoles et professionnels
- programmes de perfectionnement des athlètes
- programmes de mise en valeur et d'information

E. PARTICIPATION DU CISL

Les membres du CISL ont été appelés à deux reprises à apporter leur participation au Comité de reconnaissance des disciplines sportives.

Vous trouverez aux pages suivantes en date d'octobre 1982, les résultats du premier questionnaire.

Les membres ont également été priés de faire connaître leurs réactions au premier rapport du comité de reconnaissance (première ébauche du rapport, 20 septembre 1982). Cinq réponses ont été reçues.

(RAPPORT DU COMITE DE RECONNAISSANCE DES
DISCIPLINES SPORTIVES - Avril 1983)

OCTOBRE 1982

Annexe A

COMITE FEDERAL-PROVINCIAL DE RECONNAISSANCE
DES DISCIPLINES SPORTIVES

Sommaire des résultats - Questionnaire

1. Votre gouvernement a-t-il une politique officielle énonçant les conditions nécessaires pour qu'une discipline sportive soit reconnue? OUI - 9 NON - 2
2. Votre gouvernement a-t-il une politique officielle énonçant les traits distinctifs ou les qualités qu'une activité doit posséder pour pouvoir être reconnue comme discipline sportive? OUI - 6 NON - 5
3. Dans quelle mesure un gouvernement provincial ou territorial doit-il appuyer une discipline sportive pour que le gouvernement fédéral la considère comme étant "reconnue" dans une province donnée?

AUCUN CONSENSUS
MANIFESTE.

Beaucoup de répondants ont fait savoir que si le gouvernement provincial ou territorial reconnaît une discipline, ce critère devrait suffire. On s'oppose généralement à des calculs simples et rudimentaires comme le degré d'aide financière accordée par la province.

4. A votre avis, serait-il souhaitable d'établir des critères communs pour toutes les provinces et tous les territoires comme condition minimale de reconnaissance par le gouvernement? OUI - 7 NON - 4

5. Votre gouvernement verrait-il d'un bon oeil le fait que le gouvernement fédéral, afin de déterminer les disciplines qu'il devrait reconnaître, fixe des conditions minimales pour qu'une discipline sportive soit reconnue au sein d'une province ou d'un territoire?

OUI - 6 NON - 5

(Les réponses ne sont pas claires - certains préconisent que les provinces s'entendent entre elles pour établir des critères, tandis que d'autres concèdent au gouvernement fédéral le droit de déterminer des critères à ses propres fins.)

CA1
Z 4
-C 52

CE DOCUMENT EST EGALEMENT DISPONIBLE EN FRANCAIS

DOCUMENT: 870-112/030

Government
Publications

MEETING OF THE INTERPROVINCIAL
SPORT AND RECREATION COUNCIL

Review of Sport Canada Activities

Federal



Ottawa, Ontario
April 20, 1983

April 20th 1983

REVIEW OF SPORT CANADA ACTIVITIES

A REPORT TO THE INTER-PROVINCIAL SPORT AND RECREATION COUNCIL

HOSTING POLICY

After approval by Cabinet in the late Fall of 1982, the federal government policy on the staging of international single and multi sport events in Canada has been published. Copies will be circulated to national sport organizations, provincial-territorial governments and to prospective organizing committees. Ken Porter of Sport Canada's High Performance Unit is responsible for the administration of the hosting program, and for providing consultation and information to national bodies and/or organizing committees involved with specific events.

Sport Canada will endeavour to keep individual provinces apprised of any possible hosting application involving a specific province, and provincial officials are asking to similarly advise Sport Canada ^{of} any bid intentions.

HIGH PERFORMANCE SPORT CENTRES

A draft of the Policy document on High Performance Sport Centres has been circulated to provinces-territories for reaction purposes. Assuming that feedback through the ISRC is received at the April ISRC meeting, it is anticipated that the Policy will be finalized and available for circulation by mid-June 1983. Sport Canada is continuing to receive "applications" for training centres from individuals, national sport governing bodies, local clubs, universities, provincial governments etc. It is imperative that the Policy and accompanying Guideline documents be completed as soon as possible so that the national sport governing bodies can be established as the primary point of contact.

Jim Shaw of Sport Canada's High Performance Unit is responsible for the Sport Centres program. He will be visiting existing Centres and other available facilities during the coming year for the purpose of compiling an "inventory" of possible Centre locations. No negotiations will take place during these visits, but provinces/territories will be apprised of the proposed itinerary.

Given available financial resources, it is expected that approximately 6-8 new Centres will be established during 1983-84.

1988 "BEST EVER" PROGRAM

As part of the federal government strategy for involvement in the 1988 Calgary Winter Olympics, a plan was prepared for the development of Canada's "best ever" Winter Olympic Team. The proposal was contained in the major Cabinet Memorandum considered by Cabinet in May-June 1982.

The concept received favourable consideration and funds were provided in late February 1983 for the initial 4 years of a 5 year program. \$ 21 million dollars (1983 dollars) has been allocated for the program - the total cost over the full 5 years is slightly in excess of \$ 25 million.

In anticipation of the funding commitment, Sport Canada staff initiated a detailed planning process with each of the 10 Winter Olympic sports for the purpose of preparing comprehensive 5 year plans leading up to 1988.

As the federal and provincial Ministers agreed in the Fall 1981 Ministers' Conference that preparation for 1988 should be a sport priority, means have been sought to share the Winter Olympic sport plans with the provinces-territories. Discussions have occurred through the medium of the High Performance Blue Print Committee and mechanisms for provincial-territorial involvement will be discussed at the July meeting of the Blue Print Committee.

While some sports will take a strictly "hot housing" approach to the development of athletes for 1988, most of the sports are proposing a broader range of sport development activity and these plans will be of greater interest to the provinces-territories.

The Canadian Olympic Association has been apprised of federal plans for the "best ever" program, and co-ordination on an informal basis has been established with the COA. The COA AGM (to be held April 22-23 1983) will direct attention to more formalized co-ordination among the federal government, national sport organizations and the COA.

1984 PREPARATIONS

Although a major focus has already been placed on the 1988 Olympics, much of Sport Canada's energy is being directed to activities related to the preparation of athletes for the 1984 Winter and Summer Olympics. In general, Sport Canada has focussed its financial resources on pre-Olympic preparation, and some supplementary funding will be provided to ensure that Olympic "point-getting" prospects (mainly A & B card athletes) are able to undertake optimal preparation in the final period leading up to Sarajevo and Los Angeles.

1983-84 PRIORITIES

There are three major international Games events during 1983-84, and Sport Canada along with national governing bodies are directing their attention to these events - FISU Games (July-Edmonton), Pan Ams (August-Caracas), and Winter Olympics (February-Sarajevo). Because of these major international commitments in this fiscal year, only limited expansion in domestic programs has been feasible.

In view of the results of the High Performance Sport Task Force (preliminary report circulated at last June's ISRC Meeting), work has been undertaken with two major national sport service agencies with a view to better servicing national sport requirements. These initiatives include the following:

- Sport Medicine Council of Canada

(Planning for the creation of a joint national office incorporating staff and program operations of the Council and the four "provider" groups which provide and co-ordinate medical, para-medical and sport science services - CASS, CASM, CATA, CPA-SPD.)

- Coaching Association of Canada

(Planning for an enhanced focus on the development of coaching as a profession in Canada; and, a greater role by the CAC in special preparation of coaches involved in major international competition - e.g. Winter Olympic Coaches Seminar, concentration on Levels IV and V etc.)

NATIONAL CHAMPIONSHIPS FUNDING FORMULA

In June 1982, provinces-territories received copies of the formula used to determine funding for national championships in sports supported by Sport Canada. A few revisions have occurred and this information will be distributed to provinces-territories in mid-May. There are two problem areas at the present time: (1) funding for team sport championships in cases where all provinces and territories are represented at the national championships; and, (2) national championships for women in sports where the participation by females now warrants a national championship event.

CA1
Z 4
-C 52

DOCUMENT: 870-112/030

Traduction du Secrétariat

REUNION DU CONSEIL INTERPROVINCIAL
DU SPORT ET DES LOISIRS

Etude des activités de Sports Canada

Gouvernement fédéral



Ottawa (Ontario)
Le 20 avril 1983

Le 20 avril 1983

ETUDE DES ACTIVITES DE SPORTS CANADA

RAPPORT AU CONSEIL INTERPROVINCIAL DU SPORT ET DES LOISIRS

LA POLITIQUE D'ACCUEIL

La politique du gouvernement fédéral relative à l'organisation de compétitions internationales pour plusieurs sports ou un seul a été rendue publique après avoir été approuvée par le Cabinet à la fin de l'automne de 1982. Des copies de cette politique seront distribuées aux organisations sportives nationales, aux gouvernements provinciaux et territoriaux ainsi qu'aux comités organisateurs éventuels. Ken Porter, du Service de haute performance de Sports Canada, est chargé de l'administration du programme d'accueil et de la prestation des services de consultation et d'information aux organismes nationaux et aux comités organisateurs qui s'intéressent à des manifestations précises.

Sports Canada s'efforcera de tenir toutes les provinces au courant des demandes d'accueil touchant l'une d'elles et les fonctionnaires provinciaux sont également priés de faire connaître à Sports Canada tout projet de soumission.

LES CENTRES POUR LE SPORT DE HAUT CALIBRE

Une ébauche de l'énoncé de principes sur les Centres pour le sport de haut calibre a été distribuée à toutes les provinces et aux territoires afin de connaître leurs réactions. En supposant que le CISL ait recueilli toutes les observations à sa réunion d'avril, on pourrait mettre la politique au point de façon à être en mesure de la diffuser vers le milieu de juin de 1983. Sports Canada reçoit toujours des "demandes" visant les centres d'entraînement qui lui sont adressées par des particuliers, des organismes nationaux de régie des sports, des groupes locaux, des universités, des gouvernements provinciaux et autres. Il est impératif de mettre au point la politique et ses lignes directrices aussitôt que possible afin que les organismes nationaux de régie des sports deviennent le principal point de contact.

Jim Shaw, du Service de haute performance de Sports Canada, est chargé du programme des centres sportifs. Au cours de la prochaine année, il visitera les centres et les autres installations actuelles afin de dresser une liste des endroits où l'on pourrait établir d'autres centres. Aucune négociation n'aura lieu au cours de ces visites, mais les provinces et territoires seront informés de l'itinéraire prévu.

Les ressources financières permettent de prévoir qu'entre 6 et 8 nouveaux centres seront ouverts au cours de l'année 1983-1984.

LE PROGRAMME POUR REUNIR LA MEILLEURE EQUIPE JAMAIS VUE POUR 1988

Un des éléments de la stratégie du gouvernement fédéral en vue des Jeux olympiques d'hiver qui auront lieu à Calgary en 1988 est un plan destiné à réunir la meilleure équipe canadienne jamais vue à des Jeux olympiques d'hiver. Le projet était contenu dans l'important mémoire du cabinet étudié par ce dernier en mai et juin 1982.

L'idée a été accueillie favorablement et des crédits ont été accordés à la fin de février 1983 pour les quatre premières années d'un programme quinquennal. Ce programme se voit ainsi octroyer 21 millions de dollars (valeur de 1983) alors que son coût total sur une période de cinq ans, dépassera légèrement 25 millions de dollars.

En prévision de la réception de ces crédits, le personnel de Sports Canada a élaboré des plans détaillés pour chacun des dix sports olympiques d'hiver afin d'établir des plans quinquennaux en prévision de 1988.

Les ministres fédéral et provinciaux ayant convenu à leur conférence de l'automne 1981 que les préparatifs pour 1988 doivent constituer une priorité en matière de sport, on a cherché à intéresser les provinces et les territoires aux plans pour les Jeux olympiques d'hiver. Le Comité du plan directeur pour le sport de haut calibre a servi de carrefour aux discussions et l'on traitera de nouveau des mécanismes de participation des provinces et des territoires au cours de la réunion de ce comité qui aura lieu en juillet.

Certains sports s'en tiennent rigoureusement à la méthode du "vase clos" pour le perfectionnement des athlètes pour 1988 mais la plupart des sports proposent une gamme d'activités de perfectionnement sportif plus large, plans qui revêtent un plus grand intérêt pour les provinces et territoires.

L'Association olympique canadienne a été informée des plans fédéraux dans le cadre du programme visant à réunir la meilleure

équipe jamais vue et une coordination non officielle a été établie avec elle. Au cours de l'assemblée générale annuelle de l'AOC (qui aura lieu les 22 et 23 avril 1983), il sera question d'une coordination plus officielle entre le gouvernement fédéral, les organisations sportives nationales et l'Association olympique canadienne.

LES PREPARATIFS POUR 1984

Bien qu'une grande importance soit accordée aux Jeux olympiques de 1988, Sports Canada investit également beaucoup d'énergie dans la préparation des athlètes en vue des Jeux olympiques d'hiver et d'été de 1984. En règle générale, Sports Canada a concentré ses ressources financières sur les activités préparatoires aux Jeux olympiques et des fonds supplémentaires seront injectés pour faire en sorte que les candidats aptes à mériter des points aux Jeux olympiques (principalement les athlètes inscrits dans les catégories A et B) puissent pousser leur entraînement à son niveau optimal au cours de la période précédant immédiatement les jeux de Sarajevo et de Los Angeles.

LES PRIORITES POUR 1983-1984

Trois principaux Jeux internationaux doivent avoir lieu au cours de 1983-1984. Sports Canada et les organismes nationaux de régie des sports s'intéressent plus particulièrement à ces manifestations, qui sont les Jeux de la F.I.S.U. (en juillet à Edmonton), les Jeux panaméricains (en août à Caracas) et les Jeux olympiques d'hiver (en février à Sarajevo). En raison de ces importants engagements internationaux au cours de l'année financière, il a fallu restreindre l'élargissement des programmes nationaux.

A la lumière des conclusions du Groupe d'étude sur le sport de haut calibre (rapport préliminaire distribué à la réunion du CISL qui a eu lieu en juin dernier), des travaux ont été entrepris avec deux importants organismes nationaux de services sportifs afin de chercher à mieux répondre aux besoins des sports nationaux. Ces démarches sont les suivantes:

- Conseil canadien de la médecine sportive

(Planifier la création d'un bureau national mixte regroupant du personnel et des éléments du programme du Conseil et des quatre groupes qui fournissent et coordonnent les services médicaux, paramédicaux et scientifiques dans le domaine du sport - ACSS, ACMS, ACTS, DPS - ACP).

- Association canadienne des entraîneurs

(Planifier la mise en valeur de la profession d'entraîneur au Canada et une participation plus grande l'ACE à la préparation spéciale des entraîneurs qui participent aux principales épreuves internationales par exemple des colloques pour les entraîneurs aux Olympiques d'hiver, accent sur les niveaux IV et V, etc.).

LA FORMULE DE FINANCEMENT DES CHAMPIONNATS NATIONAUX

En juin 1982, les provinces et les territoires recevaient une copie de la formule utilisée pour calculer les subventions versées aux championnats nationaux des sports qu'appuie Sports Canada. De légères modifications ont été apportées à cette formule et les nouveaux renseignements seront distribués aux provinces et aux territoires au milieu du mois de mai. Deux secteurs font actuellement problème: 1) le financement des championnats de sports par équipe lorsque toutes les provinces et les territoires participent aux championnats nationaux; et 2) les championnats nationaux de sports pour femmes lorsque la participation de celles-ci est telle qu'elle justifie la tenue d'un championnat national.

CA1
Z 4
-002

Publication

MEETING OF THE INTERPROVINCIAL
SPORT AND RECREATION COUNCIL

REUNION DU CONSEIL INTERPROVINCIAL
DU SPORT ET DES LOISIRS

Ottawa
April 19-20, 1983

Ottawa
les 19 et 20 avril 1983

LIST OF PUBLIC DOCUMENTS

LISTE DES DOCUMENTS PUBLICS

DOCUMENT NO. ° DU DOCUMENT	SOURCE ORIGINE	TITLE TITRE
70-112/029	Federal Fédéral	Report of the Committee on Sport Recognition Rapport du comité de reconnaissance des disciplines sportives
70-112/030	Federal Fédéral	Review of Sport Canada Activities Etude des activités de Sports Canada



CA1
Z 4
-C 52

DOCUMENT: 870-112/038

Gouvernement
Publications

MEETING OF THE INTERPROVINCIAL
SPORT AND RECREATION COUNCIL

REUNION DU CONSEIL INTERPROVINCIAL
DU SPORT ET DES LOISIRS

Ottawa
April 19-20, 1983

Ottawa
les 19 et 20 avril 1983

LIST OF PUBLIC DOCUMENTS

LISTE DES DOCUMENTS PUBLICS

DOCUMENT NO. ° DU DOCUMENT	SOURCE ORIGINE	TITLE TITRE
0-112/029	Federal Fédéral	Report of the Committee on Sport Recognition Rapport du comité de reconnaissance des disciplines sportives
0-112/030	Federal Fédéral	Review of Sport Canada Activities Etude des activités de Sports Canada



870-123-001

CA1
Z4
C52

Conference on Privacy: Initiatives for 1984

Program



Dear Delegate:

I am pleased that you have been able to attend the "Conference on Privacy: Initiatives for 1984". As I indicated earlier I believe the protection of personal information in both public and private sectors is an important issue. It is perhaps doubly important because of the rapid development of new technologies confronting society today and the implications this has for the individual.

I welcome your participation and am pleased to have this opportunity to provide a forum for the private sector to make their views known and to also air the important issues surrounding the topic. Hopefully, this will act as a catalyst for the future.

As you are undoubtedly aware this symposium will be followed by an interprovincial meeting of Ministers which will examine the possible options as outlined in the Discussion Paper.

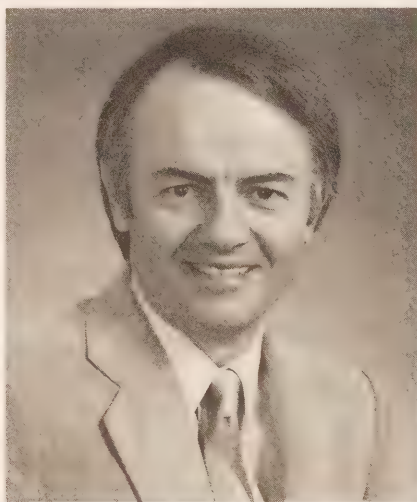
The views that are aired during the two day session will be presented to the Ministers and will form an important part of our discussions and any resolutions reached.

I trust that you find the Conference stimulating. If you wish to submit any further views after the Conference I shall be glad to receive them.

Yours sincerely,

Norman Sterling

Norman W. Sterling, Q.C.
*Provincial Secretary for
Resources Development*



"CONFERENCE ON PRIVACY: INITIATIVES FOR 1984"

SYMPOSIUM

Sponsored by

THE HONOURABLE NORMAN STERLING, O.C.

Provincial Secretary for
Resources Development

Ontario

May 22 to 24, 1984

Sheraton Centre

123 Queen Street West
Toronto, Ontario
M5H 2M9

PURPOSE

The purpose of this Symposium is to discuss the major issues connected with informational privacy in both public and private sectors.

The views of the private sector, in particular, are being sought to determine a course for the future.

PROGRAM

Tuesday, May 22

7:00 p.m. – 9:00 p.m. / Reception

Civic Ballroom – Sheraton Centre

Host: *The Honourable Norman Sterling, Q.C.*

Wednesday, May 23

8:00 a.m. – 9:00 a.m. / Registration

9:00 a.m. – 9:45 a.m. / Opening of the Symposium

Dominion Ballroom, with a keynote speech by the Honourable Norman Sterling, Q.C.

9:45 a.m. – 11:15 a.m. / Choice of two panels

Private Sector Panel: "Privacy: The Problems Defined" – Dominion Ballroom

Chairman: *Jake Knoppers*, Senior Vice-President, Informan Inc., Ottawa

Speakers: *J. Kirschbaum*, President, Fireman's Fund of Canada Limited

(representing The Insurance Bureau of Canada) Toronto

Dr. William R. Ghent, Chairman, Council on Health Care, The Canadian Medical Association, Ottawa

Ross McFarlane, Q.C., General Counsel, General Motors of Canada Limited

(representing The Canadian Manufacturers Association) Toronto

Commentator: *Professor Peter Burns*, Dean, Faculty of Law, University of British Columbia, Vancouver

Public Sector Panel: "Access to Information: How Does this Relate to Privacy?" – City Hall Room

Chairman: *Don Rowat*, Department of Political Science, Carleton University, Ottawa

Speakers: *John McCamus*, Dean, Osgoode Hall Law School, York University, Toronto

Professor David Flaherty, Privacy Project, University of Western Ontario, London, Ontario

Murray Rankin, Faculty of Law, University of Victoria

Commentator: *Ken Rubin*, Information Consultant/Researcher, Ottawa

11:15 a.m. – 12:00 noon / Break for Discussion

12:00 noon – 2:00 p.m. / Luncheon for all Delegates – Civic Ballroom

2:00 p.m. – 2:30 p.m. / Address – Dominion Ballroom

Speaker: *Dr. John Grace*, Federal Privacy Commissioner

Topic: "The Privacy Act: How Is It Working to Date"

2:30 p.m. – 3:45 p.m. / Choice of two panels

Private Sector Panel: "Privacy: What the Private Sector Has Done" – Dominion Ballroom

Chairman: *David Flaherty*

Speakers: *Ralph Hancox*, President, Readers Digest Association of Canada, Montreal

Robert G. Logan, Director, External Programs, IBM Canada Limited, Toronto

Eric Wimberley, Canadian Cable TV Association, Ottawa

Commentator: *Mel Fruitman*, Retail Council of Canada,

(Representing Payment Alternatives Communications Exchange), Toronto

Public Sector Panel: "Privacy: Some Practical Solutions" – City Hall Room

Chairman: *Jacques Fremont*, Research Centre for the Study of Public Law, University of Montreal

Speakers: *Hugh O'Neill*, President, American Society of Access Professionals, Washington, D.C.

Caroline Pestieau, Commission d'accès à l'information du Québec

Douglas Smith, Assistant Deputy Minister, Communications Policy Branch, Department of Justice,
Province of Saskatchewan

Commentator: *Mr. Bill Atkinson*, Avocat, Drouin and Associates, Quebec City

3:45 p.m. – 4:00 p.m. / Coffee

4:00 p.m. – 5:30 p.m. / All Delegates

Panel: "Privacy: Initiatives for the Private Sector" – Dominion Ballroom

Chairman: *Ed Finn*, Canadian Union of Public Employees, Ottawa

Speakers: *Maryon Brechin*, Consumers' Association of Canada, Ottawa

W. H. Loewen, President, Canadian Independent Computer Services Association, Winnipeg

Boris Mather, Canadian Federation of Communications Workers, Ottawa

Evening – Delegates Free

Thursday, May 24

9:00 a.m. – 9:45 a.m. / Address – Dominion Ballroom

Speaker:

The Honourable David Waddington, Q.C.

Minister of the State for the Home Office, United Kingdom

Topic: "Protection of Personal Information in the U.K.: The Data Protection Bill"

9:45 a.m. – 11:30 a.m. / All Delegates

Panel: "Transborder Data Flow: Toward a Resolution for the Future: The Trends, The Issue" – Dominion Ballroom

Chairman: *Russell Pipe*, President, Transnational Data Reporting Services Inc., Washington/Amsterdam

Speakers: *Professor Tom McPhail*, Graduate Program in Communications Studies, University of Calgary, Calgary

Jan Fedorowicz, Canadian Representative, International Chamber of Commerce, Ottawa

Jim Grant, Vice President Retail Banking, Royal Bank of Canada, Montreal

Commentator: *W. H. Montgomery*, Director-General, International Relations Branch,
Canadian Department of Communications, Ottawa

11:30 a.m. / Summing up of Conference by Rapporteur.

Official Closing of Symposium by Minister.

Eric G. Wimberley

M. Wimberley est vice-président - Affaires de l'association, de l'Association canadienne de télévision par câble à Ottawa. Avant de travailler dans le secteur de la télévision par câble, il a poursuivi pendant quinze ans une carrière de cadre supérieur avec Computing Devices Canada Limited et Leigh Instruments Avionics Division.

Hugh O'Neill

M. O'Neill a été l'agent de la loi sur les renseignements personnels et les pratiques loyales en matière d'information auprès du Department of Health and Human Services, à Washington, D.C., depuis que le Privacy Act est entré en vigueur en 1975. Il a représenté le ministère dans divers groupes de travail institués par le personnel du President's Domestic Policy pour étudier les recommandations de la commission

d'études sur la protection de la vie privée et a travaillé avec le personnel du President's Privacy Initiatives et autres composants du ministère à l'élaboration de nouveaux textes de loi sur la question de la protection de la vie privée. Il est également président de l'American Society of Access Professionals.

Caroline Pestiau

Mme. Pestiau a été nommée en décembre 1982 Commissaire de la commission d'accès à l'information du Québec. Elle est responsable du bureau de la commission à Montréal. Membre de la commission Pare sur l'accès des citoyens aux renseignements détenus par le gouvernement et sur la protection des données personnelles qui a soumis son rapport en mai 1981, elle était déjà très au fait d'un bon nombre des questions étudiées par la commission d'accès à l'information. Elle a fait ses études à l'université d'Oxford (M.A. en histoire contemporaine), l'université catholique de Louvain (B.A. en philosophie) et McGill University (M.A. en économie).

Douglas D. Smith

M. Smith, actuellement sous-ministre adjoint à la direction des politiques en matière de communications du ministère de la justice de la Saskatchewan, a occupé les postes suivants: sous-ministre adjoint à la section des téléphones du gouvernement du Manitoba; sous-ministre des services d'information et des communications du gouvernement du Manitoba; administrateur de Francis Williams and Johnson, experts - conseils en communication à Calgary et Edmonton; et vice-président de McConnell, Stevenson and Kellog au siège social de Winnipeg pour l'Ouest du Canada.

Maryon Brechin

Mme. Brechin, ancienne présidente de l'Association du consommateur du Canada, a consacré sa vie à la défense des consommateurs. Elle a joué un rôle actif dans l'association pendant plus de 30 ans. En 1975, elle a été nommée membre de l'Ordre du Canada pour sa remarquable contribution aux affaires des consommateurs. Elle est actuellement vice-présidente du Conservation Council of Ontario et elle représente l'Ontario au comité Codex Alimentarius de l'Organisation pour l'alimentation et l'Agriculture de l'Organisation mondiale de la santé.

W. H. (Bill) Loewen

M. Loewen est président fondateur de Comcheq Services Limited, compagnie instituée pour fournir des services informatiques de paie aux compagnies. C'est un expert-comptable qui a occupé pendant la plus grande partie de sa carrière des postes de gestion financière dans le secteur privé. Il a joué un rôle important dans les secteurs des services informatiques comme membre fondateur de la Canadian Independent Computer Services Association dont il est actuellement le président (1983-1984). Il prend également une part active à la vie de la collectivité et est membre du comité de levée de fonds de l'orchestre symphonique de Winnipeg.

Boris Mather

M. Mather s'occupe d'affaires syndicales depuis de nombreuses années. Avant 1973, il était directeur canadien de la Communications Workers of America (AFL-CIO). Il est actuellement président de la Canadian Federation of Communications Workers, fédération de 50 000 membres qui regroupe trois syndicats canadiens, à savoir le Canadian Office Employees Union, Le Syndicat des travailleurs en communication du Canada et le Syndicat des travailleurs en télécommunication.

Thomas L. McPhail, Ph.D.

M. McPhail est professeur en communications et directeur du programme de troisième cycle des études en communications de l'université de Calgary. Il a travaillé pour le ministère fédéral des politiques et d'export-comptable; il a pris part au premier projet d'interaction par câble d'Amérique du Nord avec la compagnie Miltre Corporation à Washington, D.C. et il a exercé les fonctions d'expert principal de l'UNESCO à Paris à la fin des années 1970. Il a présenté plus de 80 comptes rendus de travaux de recherche sur plusieurs aspects des communications et a publié aux éditions Sage: *Electronic Colonialism: The Future of International Broadcasting and Communication*.

Jan K. K. Fedorowicz, Ph.D.

M. Fedorowicz occupe actuellement le poste de Directeur - Politiques internationales, de la Chambre de commerce du Canada. Il est notamment en charge des réunions et de l'ordre du jour du comité sur le passage des données au-delà des frontières de l'International Business Council of Canada, ce qui l'a amené à faire des recherches, à rassembler une documentation et à préparer des exposés de principes sur le sujet. Il a écrit deux livres ainsi qu'un nombre considérable d'articles, de brochures et de commentaires. Il est directeur associé de l'institut canadien des affaires internationales depuis 1982.

William Atkinson

M. Atkinson a travaillé comme avocat pour le compte du gouvernement du Québec de 1975 à 1983. Il a pris part à la rédaction du Bill 65 du Québec sur l'accès aux documents détenus par les organes publics et la protection des données personnelles. M. Atkinson exerce actuellement à titre privé avec Drouin et associés dans la ville de Québec.

Peter Burns

Le professeur Burns a une licence et une maîtrise de droit de l'université Otago de Nouvelle-Zélande. Il a été avocat auprès de la Cour suprême de Nouvelle-Zélande avant de venir au Canada. Il a joué un rôle actif dans un grand nombre d'organisations, notamment l'Association du barreau canadien et il a travaillé comme expert-conseil. C'est le doyen de la faculté de droit de l'université de Colombie-Britannique et il a beaucoup publié dans le domaine du droit, en particulier des travaux sur la protection de la vie privée et des renseignements personnels.

COMMENTATEURS

J. C. Grant

M. Grant est ingénieur de profession et, avant de se joindre à la Banque Royale du Canada en 1968, a travaillé comme ingénieur sur les questions de contrôle du trafic aérien pour le compte du gouvernement fédéral et dans le domaine des systèmes pour une grande compagnie pétrolière. Il est actuellement vice-président - Planification stratégique, des services de détail de la Banque Royale. Il fait partie d'un nombre considérable d'organisations et c'est le délégué canadien à Paris de la commission internationale des charnières de commerce sur les politiques en matière de communication et d'information. Il est membre du conseil consultatif international de Transnational Data Report (Amsterdam) et membre du comité sur la stratégie des paiements de l'Association des banquiers canadiens.

PARTICIPANTS À LA CONFÉRENCE

CONFÉRENCIERS PRINCIPAUX

L'honorable

Norman Sterling, c.r.

M. Sterling, député de Carleton-Grenville détient également une licence en génie civil de l'Université Carleton. Il est diplômé de la faculté de droit de l'Université d'Ottawa (1969). Elu député pour la première fois en 1977, il a été nommé ministre sans portefeuille le 10 avril 1981. Il a été nommé Secrétaire provincial à la Justice le 3 février 1982 et Secrétaire provincial au Développement des ressources le 6 juillet 1983. C'est le ministre responsable des lois sur la protection des renseignements personnels et l'accès à l'information.

M. David Waddington, c.r.,

Royaume-Uni

M. Waddington, M.P. (Ribbles Valley) est le ministre d'Etat pour les affaires intérieures responsable des questions d'immigration, de nationalité, des relations communautaires, de services bénévoles et de protection des renseignements personnels. Il s'occupe actuellement de faire adopter le projet de loi sur la protection des données personnelles au parlement. Le projet devrait prendre force de loi au cours de l'été prochain.

Dr. John Grace

M. Grace est un ancien membre du Conseil de la radiodiffusion et des télécommunications canadiennes. Auparavant, il a travaillé pour *The Ottawa Journal* où il s'est acquitté de diverses fonctions avant d'en devenir président et rédacteur en chef de juin 1979 à août 1980. Il a été nommé par le parlement Commissaire à la protection de la vie privée aux termes de la Loi sur l'accès à l'information et la Loi sur la protection des renseignements personnels en juin 1983.

PRÉSIDENTS

Jacques Frémont

M. Frémont, membre du barreau québécois depuis 1978, est actuellement professeur associé en droit public à la faculté de droit de l'Université de Montréal. De 1978 à 1980, il a préparé sa thèse de doctorat à la London School of Economics and Political Science sur le contrôle judiciaire des documents administratifs contendants dans une perspective comparative. Il termine actuellement sa thèse.

Ed. Finn

M. Finn, journaliste depuis quinze ans, après avoir été expert-conseil aux relations publiques du Conseil du Travail du Canada, est directeur des relations publiques de la Fraternité canadienne des cheminots, employés des transports et autres ouvriers, et occupe actuellement le poste d'agent principal des relations publiques du Syndicat canadien de la fonction publique.

Jake Knoppers

M. Knoppers, qui vit à Ottawa, se spécialise depuis de nombreuses années dans le domaine de la technologie de l'information et des politiques en la matière. Il est vice-président principal de Inform Inc., compagnie qui se spécialise dans les services de gestion de l'information.

Don Rowat

Le professeur Rowat est membre du département de sciences politiques à l'Université Carleton. C'est un expert international sur la législation en matière de liberté d'information et sur le rôle et la fonction des ombudsmans de différentes instances. Il a écrit et publié de nombreux ouvrages sur le sujet, en particulier *Administrative Secrecy in Developed Countries* (Macmillan, Londres, 1979).

David Flaherty

David Flaherty est professeur d'histoire et de droit à l'université Western Ontario de London, Canada. C'est un expert international sur la protection de la vie privée et l'auteur de *Privacy and Government Data Banks. An International Perspective* (1979), ainsi que d'autres études. Il termine actuellement un projet de recherche de trois ans sur le manière dont fonctionnent, dans six pays différents, les lois sur la protection des renseignements personnels dans le secteur public.

G. Russell Pipe

M. Pipe est président de l'International Business Action Centre (IBAC) à Amsterdam, Hollande, et président de Transnational Data Reporting Services Inc., Amsterdam et Washington, D.C. M. Pipe assume des fonctions d'expert-conseil, de rédacteur et de conférencier et a apporté une aide précieuse à Barry Goldwater et au Senate Government Committee pour la préparation du Privacy Act (loi sur la protection des renseignements personnels) édicté en 1974. Il est rédacteur en chef de *Transnational Data Report*, publié par North Holland Publishing (Amsterdam).

MEMBRES DE LA TRIBUNE

James L. Kirschbaum

M. Kirschbaum est président et administrateur en chef de la compagnie d'assurance Fireman's Fund au Canada. Il s'est joint à la compagnie à San Francisco en 1949. Il est actuellement membre du conseil d'administration du Bureau d'assurance du Canada, du Centre for Study of Insurance Operations et de l'Insurance Advisory Organization. Il est administrateur de la Fireman's Fund Insurance Company of Canada et d'American Express Canada, Inc.

Dr. William R. Ghent

Le docteur Ghent est chirurgien à Kingston, Ontario, et président de la commission sur les soins de santé de l'Association médicale canadienne. Le docteur Ghent a fait partie de nombreuses commissions dans les hôpitaux et les universités et a beaucoup publié dans le domaine médical.

Ross W. McFarlane, c.r.

M. McFarlane a exercé à titre privé puis comme avocat-conseil à IBM pendant onze ans. Il est actuellement avocat-conseil principal de General Motors of Canada Limited. Membre de nombreuses associations, il est actuellement président du sous-comité sur l'accès à l'information de l'Association des manufacturiers canadiens.

John D. McCamus

M. McCamus est le doyen de Osgoode Hall, faculté de droit de l'université York depuis le 1^{er} juillet 1982. Il a été directeur de recherche à la commission de l'Ontario sur la liberté de l'information et la protection des renseignements personnels. Il a beaucoup publié et est souvent invité à prendre la parole sur le sujet de l'accès à l'information et la protection de la vie privée. Il est rédacteur de *"Freedom of Information, Canadian Perspectives"* (Butterworths, 1981).

Murray Rankin

M. Rankin est professeur agrégé à la faculté de droit de l'université de Victoria en Colombie-Britannique. Le professeur Tankin a beaucoup de publications à son actif sur la liberté de l'information. Il est l'auteur de *Freedom of Information in Canada: Will the Doors Stay Shut?*, publié par le Conseil canadien de la documentation juridique. C'est un expert reconnu dans ce domaine et il a été appelé à témoigner devant le Parlement.

Ralph Hancox

M. Hancox est diplômé de la School of Modern Languages de Londres, Angleterre, et a été un Harvard Niemen Fellow en 1965-1966. Il est président de The Reader's Digest Association (Canada) Limited. Son intérêt pour les lois visant la protection des renseignements personnels porte principalement sur les effets de la commercialisation directe par courrier, de la gestion des listes de consommateurs et des conséquences des vastes fichiers automatisés nécessaires de nos jours pour les opérations commerciales.

Robert G. Logan

M. Logan est administrateur - Programmes extérieurs, de IBM Canada Limited. A ce titre, il est responsable de l'identification et de l'analyse des facteurs et tendances de la nature politique, sociale ou environnementale susceptibles d'avoir un impact sur la compagnie IBM. Il prend une part active à la vie de la collectivité et aux affaires nationales et est membre du Canadian Club de l'Empire Club et de la Chambre de commerce du Canada.

GROUPE DE TRAVAIL DU SECTEUR PUBLIC : "LA PROTECTION DES RENSEIGNEMENTS PERSONNELS : QUELQUES SOLUTIONS PRATIQUES" – Salle City Hall

Président : Jacques Frémont, Centre de recherche sur l'étude du droit public, Université de Montréal
Conférenciers : Hugh O'Neill, Président, American Society of Access Professionals, Washington, D.C.
Caroline Pesteau, Commission d'accès à l'information du Québec
Douglas Smith, Sous-ministre adjoint, Direction des politiques de communication,
Ministère de la Justice, Province de la Saskatchewan
Commentateur : M. Bill Atkinson, Avocat, Drouin et associés, Québec

15 heures 45 à 16 heures / Café

16 heures à 17 heures 30 / Pour tous les délégués

GROUPE DE TRAVAIL : "LA PROTECTION DES RENSEIGNEMENTS : INITIATIVES POUR LE SECTEUR PRIVÉ" – Salle Dominion

Président : Ed Finn, Syndicat canadien de la fonction publique, Ottawa
Conférenciers : Maryon Brechin, Association des consommateurs du Canada, Ottawa
W. H. Loewen, Président, Association canadienne des services informatiques indépendants, Winnipeg
Boris Mather, Fédération canadienne des travailleurs des communications, Ottawa

Soirée – Libre pour les délégués

Judi 24 mai

9 heures à 9 heures 45 / Discours – Salle Dominion

Conférencier :
L'honorable David Waddington, C.R.
Ministre d'état du Home Office du Royaume-Uni
Sujet : "La protection des renseignements personnels au Royaume-Uni : Le Data Protection Bill"

9 heures 45 à 11 heures 30 / Pour tous les délégués

GROUPE DE TRAVAIL : "CIRCULATION DES DONNÉES PAR TRANSBORDREUR : VERS UNE SOLUTION POUR L'AVENIR, LES TENDANCES, LE PROBLÈME" – Salle Dominion

Président : Russell Pipe, Président, Transnational Data Reporting Services Inc., Washington/Amsterdam
Conférenciers : Professeur Tom McPhail, Programme d'études supérieures en communications,
Université de Calgary, Calgary
Jan Fedorowicz, Représentant canadien, Chambre de commerce internationale, Ottawa
Jim Grant, vice-président, Banque royale du Canada, Montréal
Commentateur : W. H. Montgomerie, Directeur-général, Direction des relations internationales,
Ministère des Communications du Canada, Ottawa
Clôture officielle de l'atelier par le ministre.

11 heures 30 / Sommaire de la conférence par le rapporteur

PROGRAMME

Mardi 22 mai

19 à 21 heures / Réception

Salle Civic – Centre Sheraton

Hôte : L'honorable Norman Sterling, C.R.

Mercredi 23 mai

8 heures à 9 heures / Inscription

9 heures à 9 heures 45 / Salle Dominion

Ouverture de l'atelier par une allocution prononcée par l'honorable Norman Sterling, C.R., sur le thème de l'atelier.
9 heures 45 à 11 heures 15 / Choix de deux groupes de travail

GROUPE DE TRAVAIL DU SECTEUR PRIVÉ : "LA PROTECTION DES RENSEIGNEMENTS PERSONNELS : DÉFINITION DES PROBLÈMES" – Salle Dominion

Président : Jake Knoppers, Premier vice-président, Informan Inc., Ottawa

Conférenciers : J. Kirschbaum, Président, Fireman's Fund du Canada Limitée

(représentant le Bureau d'assurance du Canada) Toronto

Docteur William R. Ghent, Président, Conseil des soins de santé,

L'Association médicale canadienne, Ottawa

Ross McFarlane, C.R., Avocat conseil, Général Motors du Canada Limitée

(représentant l'Association des manufacturiers canadiens) Toronto

Commentateur : Professeur Peter Burns, Doyen de la faculté de droit, Université de Colombie-Britannique, Vancouver

GROUPE DE TRAVAIL DU SECTEUR PUBLIC : "ACCÈS À L'INFORMATION : COMMENT CECI SE RATTACHE-T-IL À LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ?" – Salon City Hall

Président : Don Howat, Département de Science politique, Université Carleton, Ottawa

Conférenciers : John McCamus, doyen, Faculté de droit d'Osgoode Hall, Université York, Toronto

Professeur David Flaherty, Projet sur la protection des renseignements personnels,

Université Western Ontario, London (Ontario)

Commentateur : Ken Rubin, Conseiller/chercheur en information, Ottawa

11 heures 15 à 12 heures / Pause-discussion

12 heures à 14 heures / Déjeuner pour tous les délégués – Salle Civic

14 heures à 14 heures 30 / Discours – Salle Dominion

Conférencier : Docteur John Grace, Commissaire fédéral à la protection des renseignements personnels
Sujet : "La Loi sur la protection des renseignements personnels : Ses résultats jusqu'à présent"

14 heures 30 à 15 heures 45 / Choix de deux groupes de travail

GROUPE DE TRAVAIL DU SECTEUR PRIVÉ : "LA PROTECTION DES RENSEIGNEMENTS PERSONNELS : QU'A FAIT LE SECTEUR PRIVÉ?" – Salle Dominion

Président : David Flaherty

Conférenciers : Ralph Hancox, Président, Association Readers Digest du Canada, Montreal

Robert G. Logan, Directeur des programmes externes, IBM Canada Limitée, Toronto

Eric Wimberey, Association canadienne de télévision par câble, Ottawa

Commentateur : Mel Fruitman, Conseil canadien du commerce de détail,

(représentant le Payment Alternatives Communications Exchange), Toronto

Le but de cet atelier est de discuter des principales questions portant sur la protection des renseignements personnels dans le secteur public ainsi que dans le secteur privé.
On recherchera en particulier les points de vue du secteur privé en vue d'établir des lignes de conduite pour l'avenir.

**"CONFÉRENCE SUR LA
VIE PRIVÉE :
PROJETS POUR 1984"
ATELIER**

Commandité par

L'HONORABLE NORMAN STERLING, C.R.

Secrétaire de la province au Développement
des ressources

Ontario

du 22 au 24 mai 1984

Centre Sheraton

123 ouest, rue Queen
Toronto (Ontario)
M5H 2M9

Madame,
Monsieur,

Je suis heureux que vous ayez pu venir assister à la conférence intitulée *Protection de la vie privée* : *projets pour 1984*. Au risque de me répéter, je rappelle que la protection des renseignements personnels dans les secteurs public et privé est une question importante. Son urgence est peut-être due à la rapidité avec laquelle les nouvelles technologies envahissent la société contemporaine et aux conséquences que cela risque d'avoir sur les particuliers.

Je vous remercie de votre participation et je suis heureux que le secteur privé ait cette occasion de faire connaître ses opinions tandis que ces graves questions sont librement discutées. J'espère que cette conférence servira de catalyseur pour l'avenir.

Comme vous le savez sans doute, ce symposium sera suivi d'une rencontre interprovinciale des ministres qui étudieront les diverses solutions proposées dans ce document de travail.

Les opinions qui seront exprimées au cours de ces deux jours seront présentées aux ministres et constitueront un élément important des décisions auxquelles nous parviendrons.

J'espère que vous trouverez cette conférence intéressante. Si vous désirez soumettre d'autres idées une fois la rencontre terminée, je serai à votre disposition.

Cordialement,

Norman Sterling

Le Secrétaire provincial
au Développement des
ressources

Norman W. Sterling, c.r.





**Conférence sur la vie
privée:
projets pour 1984**

Programme

INTERPROVINCIAL CONFERENCE ON PRIVACY:
INITIATIVES FOR 1984 (SYMPOSIUM)

CONFÉRENCE INTERPROVINCIALE SUR LA PROTECTION
DES RENSEIGNEMENTS PERSONNELS : MESURES POUR 1984 (COLLOQUE)

Final List of Delegates

Liste définitive des délégués



Toronto, Ontario
May 23-24, 1984

Toronto (Ontario)
Les 23 et 24 mai 1984

NOTE

Please report to the Secretariat
any inaccuracies that may appear
in this list.

NOTA

Nous vous prions de signaler
au Secrétariat toute erreur qui
peut comporter cette liste.

INTERPROVINCIAL CONFERENCE ON PRIVACY:
INITIATIVES FOR 1984 (SYMPOSIUM)

CONFÉRENCE INTERPROVINCIALE SUR LA PROTECTION
DES RENSEIGNEMENTS PERSONNELS : MESURES POUR 1984 (COLLOQUE)

TORONTO

May 23-24, 1984

Les 23 et 24 mai 1984

Final List of Delegates
Liste définitive des délégués

PARTICIPANTS

Hon. Norman Sterling
Provincial Secretary
for Resources Development

CHAIRMAN/PRÉSIDENT

Hon. David Waddington
Minister of State for the
Home Office, United Kingdom

Bill Atkinson
Avocat
Drouin and Associates
Québec City

Maryon Brechin
Consumers' Association of Canada
Ottawa

Peter Burns
Dean, Faculty of Law
University of British Columbia
Vancouver

Jan Fedorowicz
Canadian Representative
International Chamber of Commerce
Ottawa

Ed Finn
Canadian Union of Public Employees
Ottawa

David Flaherty
Privacy Project
University of Western Ontario
London, Ontario

Jacques Fremont
Research Centre for the
Study of Public Law
University of Montreal

Mel Fruitman
Retail Council of Canada
(Representing Payment Alternatives
Communications Exchange) Toronto

William R. Ghent
Chairman
Council on Health Care
The Canadian Medical Association
Ottawa

John Grace
Federal Privacy Commissioner

Jim Grant
Royal Bank of Canada
Montreal

Ralph Hancox
President
Readers Digest Association of Canada
Montreal

J. Kirschbaum
President
Fireman's Fund of Canada Limited
(Representing The Insurance Bureau of Canada)
Toronto

Jake Knoppers
Senior Vice-President
Infoman Inc.
Ottawa

W.H. Loewen
President
Canadian Independent Computer
Services Association
Winnipeg

Robert G. Logan
Director, External Programs
IBM Canada Limited
Toronto

Boris Mather
Canadian Federation of
Communications Workers
Ottawa

John McCamus
Dean
Osgoode Hall Law School
York University
Toronto

Ross McFarlane
General Counsel
General Motors of Canada Limited
(Representing The Canadian
Manufacturers Association)
Toronto

Tom McPhail
Graduate Program in Communications Studies
University of Calgary
Calgary

Hugh O'Neill
President
American Society of Access Professionals
Washington, D.C.

Caroline Pestieau
Commission d'accès à l'information du Québec

Russell Pipe
President
Transnational Data Reporting Services Inc.
Washington/Amsterdam

Murray Rankin
Faculty of Law
University of Victoria

Don Rowat
Department of Political Science
Carleton University
Ottawa

Ken Rubin
Information Consultant/Researcher
Ottawa

Douglas Smith
Assistant Deputy Minister
Communications Policy Branch
Department of Justice
Province of Saskatchewan

Eric Wimberley
Canadian Cable TV Association
Ottawa

PRIVATE SECTOR - SECTEUR PRIVÉONTARIO

Erika Abner
Canadian Civil Liberties Association

J.H.J. Aldrich
President
Registered Insurance Brokers of Ontario

Dr. A. Ameis
Ontario Medical Association

Bob Amsterdam
Amsterdam & Peroff

H. Anderson
Registered Insurance Brokers of Ontario

Maurice Anderson
Vice-President
Information Systems
Simpsons-Sears Limited

Ronald G. Atkey
Osler, Hoskin and Harcourt
Barristers and Solicitors

Rick Babyak
Arthur Anderson and Company

Irene Bailey
Canadian Association of Women Executives

Harold Ball
Intertec

Allan Bassin
Insurance Bureau of Canada

Kevin Belgrave
Executive Vice-President & General Manager
Associated Credit Bureaus of Ontario

Paul Boire
Past President
Canadian Association of Data
and Professional Services Organization

Chris Boddy
Compu-Guard System Inc.

Carne Bray
Association of Canadian
Financial Corporations

Lois N. Brebner
Bell Canada

Grace Brooker
 Director - National Office
 Canadian Information Processing Society

Paul C. Brown
 Manager
 Marketing Services
 Maclean Hunter Cable TV

Bryan Cantley
 Manager
 Editorial Services
 Canadian Daily Newspaper
 Publishers Association

Ron Chaplin
 Government Affairs Officer
 Canadian Petroleum Association

Norman Cheesman
 Director of Public Affairs
 Canadian Business Equipment Manufacturers Association

Nancy Christie
 Executive Director
 Canadian Physiotherapy Association

G.R. Clayton
 Victoria and Grey Trust

J.R. Coghill
 Manager
 Registered Insurance Brokers of Canada

Ken Cooke
Director
Insurance Operations
Canadian Life and Health
Insurance Association

W. Cooke
Toronto Credit Bureau

J.G. Crean
President
Robert Crean & Company Limited

W.R.J. Cresswell
Chairman
Computer Committee
Ontario Association of Certified
Engineering Technicians and Technologists

Elizabeth Cummings
President
Ontario Library Association

Antony Cunningham
Canadian Federation of Insurance
Agents and Brokers Association

Doug Curtis
Dofasco

Pieter de Josselin de Jong
Financial Executives Institute Canada

John Dean
Board of Trade of Metropolitan Toronto

Yves Desjardins-Siciliano
IBM Canada Limited

Jim Dingle
Deputy Chairman
Canadian Payments Association

N.C. Draper
Manager
Industrial Relations
Human Resources Department
Imperial Oil Limited

Nigel Dunn
Insurance Bureau of Canada

A.J. Dunsdon
Deputy Registrar
Ontario College of Pharmacists

Christopher Du Vernet
Blake Cassels and Graydon

Jim Dykes
President
Motor Vehicle Manufacturers Association

J.I. Eagan
Simpsons-Sears Limited

Lori Ferman
York University

Bernie E. Floyd
Director
Civic Security and Investigative Services

Larry Foerster
Barrister and Solicitor
McIntyre, Rowan and Associates

David Foster
Traders Group

R.B. Franceschini
Executive Director
Ontario Pharmacists' Association

Gary Gillam
Director
Legal and Governmental Affairs
Credit Union Central of Ontario

J.G.L. Girouard
Manager
Inter-Industry Operations
Domestic Banking
Bank of Montreal

Roy Graham

Peter S. Grant
Lawyer
McCarthy & McCarthy

Jill Greenwell
Professional Officer
Canadian Association of
University Teachers

Jack Gryfe
Chairman
Council on Hospital Services
Canadian Dental Association

Fred Hamblin
Executive Director
Association of Colleges of Applied
Arts and Technology of Ontario

Hugh Harkness
Construction Safety Association
of Ontario

Peter Harte
University of Western Ontario

Derek C. Hayes
Vice-President
General Counsel and Secretary
Shell Canada Limited

Rudy Hegele
Montreal Trust

R.E. Henry
Manager
London Life Insurance Company

Allan Hertz
Executive Editor
Computer Law

J.S. Hutton
Victoria and Grey Trust

John Hylton
Lawyer
Borden & Elliot

Bob Jarman
Counsel
Trust Division
National Trust Company

J. Jasper
Executive Vice-President
Fireman's Fund Insurance Company
of Canada Limited

Janet Kaufman
Member, Canadian Library Association
Document and Media Resources Centre
University of Guelph

J. Brent Kelman
Vice-President
Data Resources
Canada Trust

Peter Knowlton
General Council
Bell Canada

Keith Koskie
Compu-Guard System Inc.

Peter G. Laflair
The Institute of Chartered Accountants
of Ontario

J.C. Larsen
Senior Vice-President and
Senior Consumer Credit Officer
Domestic Banking Group
Bank of Montreal

Robert Lavell
 Head
 Security for Information Systems
 Royal Trust

Pat Learmonth
 Coordinator
 Telecommunications
 Canadian Bankers' Association

Lewis Lederman
 Legal Counsel
 Canadian Payments Association

Pat Leslie
 Royal Bank of Canada

Carol Lipsett
 C.I.P.S.

Norman Luker
 Northern Telecom Limited

James McCracken
 Manager
 Legal Department
 Board of Trade of Metropolitan Toronto

J. McDaniel
 Computer Ombudsman
 Canadian Information Processing Society

G. McKay
 Data Security Planner
 Operations and Systems Division
 Operations Planning Department
 Bank of Montreal

Katherine L. McLeod
The Public Interest Advocacy Centre

Duncan MacDonald
Ontario Federation of Labour

L. Mador
President
College of Physicians & Surgeons

Paul Mahoney
Vice-President and
Medical Director
Prudential Insurance Company
of America

Veronica Maidman
President
Toronto Credit Bureau

Jason Mandolitz
Canadian Federation of
Independent Business

J. Fraser Mann
Borden & Elliot
Barristers and Solicitors

Ron Mar
Vice-President
Association of Systems Management

Roman R. March
Associate Professor
Department of Political Science
McMaster University

Tanis Mathers
Consumers Association of Canada, Ontario

Denis Mazerolle
Compu-Guard Systems Inc.

Beth Miller
Past President
Ontario Library Association

Harry L. Mills
Educational Representative
School of Continuing Education
University of Toronto

John F. Mullen
Canada Trust

Neil Naft
Delphicraft Inc.

W.C. Nursey
London Life Insurance Company

D. O'Brien
Lawrence Park Collegiate Institute

R.K. Orchin
Assistant to the Vice-President
Business Systems
Northern Telecom Limited

Ian Outerbridge
Solicitor

Paul Pagnuelo
Legislation and Government Advisor
Bank of Montreal

Robert Parker
Royal Bank of Canada

I.I. Pask
Supervisor of Operations
Ontario Association of Certified
Engineering Technicians and Technologists

Winston Peace
President-Elect
Canadian Payroll Association
London

Pamela Pestaluky
Canadian Co-operative Credit Society

David Phillips
Legal Adviser
Canadian Bankers' Association

Ken Porter
Greenlite (Media)

Steve Ralph
Canadian Bar Association

Frank Reilly
Senior Legal Officer
INCO Limited

Gwennyth Roberts
Director-at-Large
(Clinical Practice)
Canadian Physiotherapy Association

Brian M. Rogers
Blake Cassels and Graydon

E. Rosinke
Ontario Association of
Professional Social Workers

Linda Routledge
Consumer Affairs Adviser
Canadian Bankers' Association

Elizabeth Sass
E.B. Sass and Company
Management Consultants

Jim Saunders
Donvon Life

Robert Sax
Super Channel

Gordon Silverton
President
Ontario Pharmacists Association

Douglas Simpson
Financial Executives Institute Canada

R.M. Snelgrove
General Counsel
Ford Motor Company of Canada Limited

Elaine Stefanie
President
Consumers Association of Canada - Ontario

D. Stewart
President
Equifax Services Limited

Keith Stodart
Northern Telecom Limited

Norman Talbot
Regional Manager
Government and Public Affairs
Household Finance Corporation of Canada

Terry Taylor
Assistant to General Manager
Insurance Brokers Association of Ontario

Michael Thurston
Legal Counsel
College of Nurses of Ontario

Dianne Townson
Bank of Commerce

B. Upjohn
Registered Insurance Brokers of Ontario

Paulette Vinette
Institute of Association Executives

Janice Wagnstaff

Rod Walsh

Alex Watters
Director
Operations Division
Canadian Bankers' Association

W. Robert Waugh
Financial Executives Institute Canada

David Weismeilleur
Belleville Public Library

Peter Wells
Lawrence Park Collegiate Institute

Sally Woodhead
Canadian Information Processing Society

QUÉBEC

J.C. Chartrand
President
Acrofax Inc.

Jean-Marie Gélinas
Manager
Data Processing
Reader's Digest Association (Canada) Ltd.

Marc LaPerriere
Law Department
Texaco Canada, Inc.

Mike Moffat
Bell Canada

Marcel Pepin
Président
Commission d'accès à l'information

Bernard Poirier
Vice-President and
Marketing Director
Reader's Digest Association (Canada) Ltd.

Pierre Trudel
Professeur
Centre de recherche en Droit public

NOVA SCOTIA - NOUVELLE-ÉCOSSE

Louis Vagianos
Executive Director
Institute for Research on Public Policy

NEW BRUNSWICK - NOUVEAU-BRUNSWICK

Harold L. Bettle
Manager
Internal Audit and Security
Information and Public Affairs
The New Brunswick Telephone Company Ltd.

Wayne Paterson
University of Moncton

MANITOBA

No representative / Aucun représentant

BRITISH COLUMBIA - COLOMBIE-BRITANNIQUE

A.I. Fisk
Director, Security Services
British Columbia Systems Corporation

Jim Quail
Solidarity Coalition

Hart Will
School of Public Administration
University of Victoria

PRINCE EDWARD ISLAND - ILE-DU-PRINCE-EDOUARD

No representative / Aucun représentant

SASKATCHEWAN

No representative / Aucun représentant

ALBERTA

David Balcon
Ourson Consulting

NEWFOUNDLAND - TERRE-NEUVE

No representative / Aucun représentant

YUKON

No representative / Aucun représentant

NORTHWEST TERRITORIES - TERRITOIRES DU NORD-OUEST

No representative / Aucun représentant

UNITED STATES - ÉTATS-UNIS

Alan Adler
Centre for National Security Studies
Washington, D.C.

Deborah Drosnin
Editor
Access Reports/FOF
Washington Monitor Inc.
Washington, D.C.

Brian N. Garrett
Director
Government Relations
Equifax Inc.
Atlanta, Georgia

Evan Hendricks
Publisher
Privacy Times
Washington, D.C.

John Thomson
M.J.T. Research
Cambridge, Mass.

Jan Henderson
Australia

PUBLIC SECTOR - SECTEUR PUBLIC

CANADA

E.W. Aumand
Coordinator
Access to Information and Privacy
Secretariat
Secretary of State

P. Banning
Director
"F" directorate
Royal Canadian Mounted Police

Jean-Claude Bouchard
Coordinator
Secretariat on Access to
Information and Privacy
Communications Canada

Réjean Brunet
Chief
Paperwork Management Division
Public Service Commission

Sharon Card
Department of the Solicitor General

Roger Côté
Access and Privacy
Transport Canada

Ruth Deakin
Coordinator
Access to Information and Privacy
National Research Council of Canada

Peter Gillis
Information Policy Section
Administrative Policy Branch
Treasury Board of Canada Secretariat

Glen Gilmour
Lawyer
Law Reform Commission of Canada

Ann Goldsmith
Office of Privacy Commissioner
Ottawa

Inger Hansen
Office of Privacy Commissioner
Ottawa

Robert J. Hayward
Chief, Access Section
Federal Archives Division
Public Archives of Canada

B. Hayes
Government of Canada
in Prince Edward Island

Stephen Heeney
 Special Advisor
 United States Branch
 Department of External Affairs

Joanne Hinchey
 Acting Head
 Access to Information and Privacy
 Supply Administration
 Department of Supply and Services Canada

Al Hurd
 Canadian Mortgage and Housing Corporation

E.G. Jamieson
 Director
 Information Access and Records Management
 Correctional Services of Canada

Pierre Lanoix
 Access Coordinator
 Supply and Services

Claude Leost
 Access Coordinator
 Canadian Mortgage and Housing Corporation

Joanne Leslie
 Office of the Legal Counsel
 Privy Council Office

Frank McDonald
 Consumer and Corporate Affairs Canada

J.P. McDonald
 Secretary of State

D. Matheson
Systems and Procedures
Employment and Immigration Canada

M. Melissen
Information Services
Department of National Defense

Ron Morin
Senior Officer
Access to Information and Privacy
Department of National Revenue
Revenue Canada, Customs and Excise

Mhoire Murdock
Privacy Coordinator
Canada Post Corporation

Richard Needham
Director
Administrative and Library Services
Labour Canada

Tim Noël
Bank of Canada

Lynn Préfontaine
Access to Information and Privacy Unit
Department of Finance

Margaret T. Regan
Access to Information and
Privacy Secretariat
Secretary of State

Peter Robinson
Consumer and Corporate Affairs Canada

Robert St. Jean
Administrative and Library Services
Labour Canada

S.J. Skelly
Assistant Deputy Minister
Legal Services
Justice Canada

Pierre Trottier
Coordinator
Access to Information and Privacy Office
Regional Industrial Expansion
Department of Industry, Trade and Commerce

Jerry Van Berkel
Office of Privacy Commissioner
Ottawa

Jill Wallace
Department of Justice

J.F. Walsh
Director
Public Rights Administration
Employment and Immigration Canada

George A. White
Director General
Personnel Coordination (Privacy)
Department of National Defense

ONTARIO

Don Stevenson
Deputy Provincial Secretary
for Resources Development

Norm Allen
Management Systems Branch
Ministry of Health

Simon Armstrong
Ministry of Labour

Linda Bohnen
Director
Investigations
The Ombudsman's Office

Loretta Bozovich
Executive Assistant to the
Provincial Secretary for Resources Development

David Cheserton

Bill Closs
Ontario Provincial Police

J.M. Dykstra
Manager
Bus Transportation Office
Transportation Regulation Development Branch
Ministry of Transportation & Communications

Nick Ferris
Provincial Secretariat for Resources Development

Helen Fritz
Legislative Assembly

Ira Greenspoon
Legal Counsel
Financial Institutions Division
Consumer & Commercial Relations

Daniel Hill
Ombudsman

Liz Johnstone

Norm Karkruff
Management Systems Branch
Ministry of Health

Lisanne Lacroix
Research Officer
Council for Franco-Ontario Affairs
Ministry of Intergovernmental Affairs

Brian Land
Director
Research and Information Services
Legislative Library

David Long
Ministry of Transportation and
Communications

Mary McDonald
Provincial Secretariat for
Resources Development

Garth McNaughton
Policy Advisor
Policy and Planning Branch
Ministry of Consumer and
Commercial Relations

G.S. Machen
Office of the Provincial Auditor

David Martin
Manager
Organization Policy
Ministry of Municipal Affairs and Housing

Eleanor Meslin
Executive Director
Ombudsman's Office

Paul Mouncey
Provincial Secretariat
for Resources Development

Elizabeth Patterson
Director
Legal Services Branch
Ministry of Revenue

Richard Puccini
Director
Communications Policy Branch
Ministry of Transportation and Communications

Donald J.M. Reid
Chief Investigator
Investigation and Policy Service
Financial Institutions Division
Ministry of Consumer & Commercial Relations

Ann Rowan
Consumer Liaison Officer
Business Practices Division
Ministry of Consumer and Commercial Relations

Blair Smith
Manager
Information Management Office
Ministry of Transportation and Communications

William W. Stoddart
Registrar
Ministry of Consumer and Commercial Relations

Bill Sulston
General Headquarters
Ontario Provincial Police

Milan Then
Communications
The Ombudsman's Office

Barry Tocher
Director
Policy and Planning Branch
Ministry of Consumer and Commercial Relations

Cyril Townsend
Director
Corporation Tax Branch
Tax Revenue Program
Ministry of Revenue

Elizabeth Warner
Provincial Secretariat for
Resources Development

Frank White
Senior Officer
Management Technology Branch
Management Board of Cabinet

Leslie Wood
IDEA Corporation

Michael Zacks
 Director
 Legal Services
 The Ombudsman's Office

QUÉBEC

Maria Sauer
 Secrétaire
 Comité de la Loi 65

Lucy Wells
 Ministère des Communications

NOVA SCOTIA - NOUVELLE-ÉCOSSE

David Colville
 Director, Communications Policy
 Department of Transportation

Randall R. Duplak
 Communications Policy Advisor
 Department of Transportation

Bev Hamm
 Deputy Minister
 Department of Transportation

NEW BRUNSWICK - NOUVEAU-BRUNSWICK

Thomas O.C. Makin
Superintendent of Insurance
Insurance Branch
Department of Justice

MANITOBA

Zorianna Hyworon
Assistant Deputy Minister
Information Management Division
Department of Industry, Trade
and Technology

Hon. Myrna Phillips
Legislative Assistant to the
Minister of Industry, Trade and Technology

BRITISH COLUMBIA - COLOMBIE-BRITANNIQUE

Aimee Botje-Jones
B.C. House, Ottawa

PRINCE EDWARD ISLAND - ILE-DU-PRINCE-ÉDOUARD

No representative / Aucun représentant

SASKATCHEWAN

Patrick Carey
 Chief of Staff
 Minister of Justice
 Department of Justice and
 Attorney General's Office

David Stuewe
 Policy Secretariat Director
 Consumer and Commercial Affairs

Greg Wensel
 Special Assistant to the
 Minister of Justice
 Department of Justice and
 Attorney General's Office

ALBERTA

Richard Dalon
 Executive Director
 Social and Cultural Affairs
 Department of Federal and
 Intergovernmental Affairs

Jim Dawson
 Senior Advisor, Telecommunications
 Department of Utilities and
 Telecommunications

Gordon Haase
 Assistant Deputy Minister
 Department of Utilities and
 Telecommunications

Ken Murrigane
 Director, Communications Policy Branch
 Department of Utilities and
 Communications

R. Reynolds
 Senior Intergovernmental Officer
 Social and Cultural Affairs
 Department of Federal and
 Intergovernmental Affairs

NEWFOUNDLAND - TERRE-NEUVE

E. Hunter Rowe
 Acting Director, Communications
 Division
 Intergovernmental Affairs Secretariat
 Executive Council

YUKON

Miriam McTiernan
 Territorial Archivist
 Yukon Archives
 Department of Tourism,
 Recreation and Cultural Resources

Andy Vantell
 Deputy Minister
 Department of Government Services

NORTHWEST TERRITORIES - TERRITOIRES DU NORD-OUEST

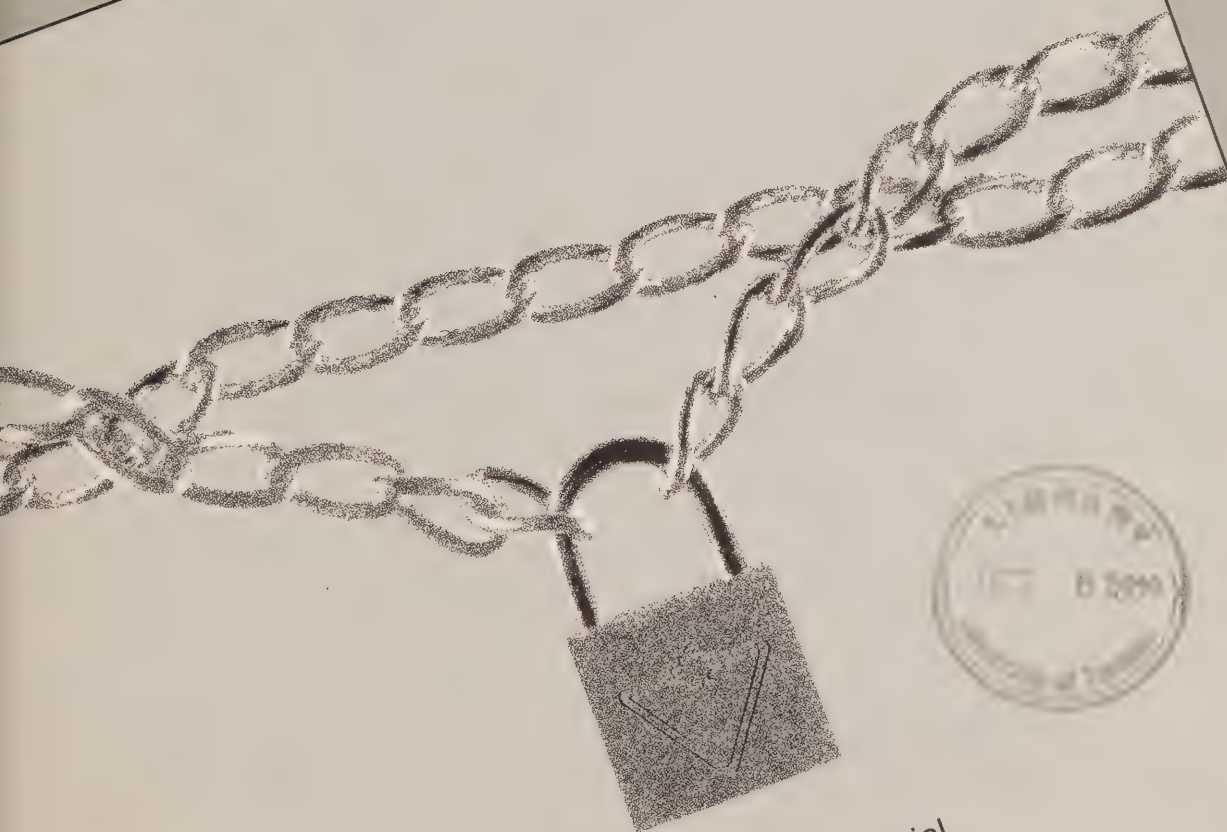
No representative / Aucun représentant

CANADIAN INTERGOVERNMENTAL CONFERENCE SECRETARIAT
SECRÉTARIAT DES CONFÉRENCES INTERGOUVERNEMENTALES CANADIENNES

Pierre-Luc Perrier
Secretary of the Conference /
Secrétaire de la conférence

041
74
052

Discussion Paper on Privacy: Initiatives for 1984



Provincial
Secretariat
for Resources
Development

The Honourable
Norman W. Sterling, Q.C.
Provincial Secretary



Provincial
Secretary for
Resources
Development

Whitney Block
Queen's Park
Toronto, Ontario
M7A 1A2
416/965-7721

MESSAGE FROM THE MINISTER:

During the last decade, concern for privacy has surfaced as one of the leading issues facing modern industrial societies. This concern has been escalated by technological innovation coupled with the growing awareness that, as citizens, we are no longer in a position where we can rely solely on our own efforts to protect personal privacy.

The right to privacy is something all of us guard closely and value highly. Ironically though, there has never been adequate legal recognition of this right in Canada.

This Discussion Paper examines various options which Governments may wish to consider when developing a response to privacy issues. It is equally important, however, that these concepts be considered in consultation with the private sector.

The importance of developing a uniform approach to this growing issue becomes readily apparent when one realizes that information gathered about an individual may be stored and actually used in another Province or Country.

Some companies in the private sector have responded to privacy concerns by developing privacy codes to govern the handling of personal information in their operations. However, companies with privacy codes are still the exception rather than the norm, suggesting that there is a need to set standards to ensure that infringements of citizens' privacy rights do not occur.

Many European countries presently have some form of Data Protection Legislation in place and, in 1981, the Council of Europe adopted a Data Protection Convention which was signed by all participating countries.

The concerns surrounding privacy and computer protection are very real. It is important, however, that these issues be addressed with industry in a coordinated and responsible manner. It is my hope that this Discussion Paper will serve as a successful first step towards achieving a Privacy Protection Code for citizens.

A handwritten signature in dark ink, appearing to read "Norman Sterling".

Norman Sterling, Q.C.
Provincial Secretary for
Resources Development

TABLE OF CONTENTS

	Page
Synopsis	iii
 PART I: UNDERSTANDING THE ISSUES	 1
Introduction	1
Fair Information Practices	4
Public Perceptions	6
Industry Response	8
 PART II: LEGISLATION GOVERNING PUBLIC SECTOR DATA BANKS	 10
Canada	10
Provinces	11
United States	12
United Kingdom	13
Federal Republic of Germany	13
Sweden	14
Council of Europe	15
Organization for Economic Cooperation and Development	15
Summary	16
 PART III: ALTERNATIVES FOR THE PRIVATE SECTOR	 18
Summary of Issues	18
Scope	20
Policy Options	21
Summary	29

SYNOPSIS

Developments in computer and telecommunications technology have raised new questions about informational privacy - the capacity for individuals to determine what information is collected about them and the manner in which it is made available to others. This Discussion Paper introduces the reader to some of the major issues raised by the potential impact of technological developments on privacy and discusses some alternative approaches to their resolution.

These issues centre on data collection, data quality, disclosure limitations, security safeguards, costs and individual access to personal records in computerized data banks. Recent surveys of public attitudes suggest that individuals are very concerned about computers affecting personal privacy and about institutions collecting too much personal information.

The public sector has begun to address these problems with various statutes which establish and enforce fair information practices for data banks held by government departments and agencies. Examples include Canada's Federal Privacy Act and Quebec's Bill 65, both of which also establish offices to ensure compliance with privacy standards and consider individual complaints regarding information practices.

Ontario is considering a proposal in its draft Privacy and Access to Information Bill that would seek to establish fair information practices for provincial government data banks. It would set up a compliance office as well as an office to receive citizens' complaints regarding information practices.

Data protection has received much attention in Europe, where countries like the United Kingdom, West Germany and Sweden have legislative programs which register data banks and regulate information practices in both the public and private sectors.

The private sector has shown sensitivity to privacy concerns by developing internal practices and, in some cases, voluntary privacy codes which embrace some of the principles commonly found in data protection laws. In the United States, Warner-Amex Cable Communications Inc. has developed a code to protect the privacy of the personal information it gathers on its customers. The Canadian Cable Television Association is in the process of developing a privacy code with similar self-regulation objectives.

Traditionally, credit bureaus, which are regulated in most provinces by credit reporting Acts, have been the main handlers of personal information in the private sector. However, the growth of computerized personal information banks can be seen in a wide range of industries including financial

institutions, cable TV services, videotex services, computer services as well as a host of other business and non-business sectors. The individual has no concrete guarantees against infringements of informational privacy in these data banks.

In order to develop a uniform approach to the privacy problem, Canadian jurisdictions will have to grapple with a number of legal issues. These include questions such as: Who owns the information in personal data banks? How should that information be legally protected? Do existing privacy laws need to be amended in light of the expanding technology? Does liability ensue from an improper or unauthorized release of personal information? Then, of course, there is the everlasting problem of jurisdiction between the federal, provincial and territorial governments to harmonize rules as they are developed and to avoid any conflicts in the laws.

It is a generally held view that individual rights, including privacy rights, are not within the exclusive legislative competence of either the Federal or Provincial levels of government but rather are determined by the Canadian Constitution and more particularly S.91 and S.92 of the B.N.A. Act. Although a number of governments already have Privacy Statutes, it is important that these initiatives continue and perhaps expand.

This paper analyzes four approaches to resolving privacy concerns brought about by the growth in computerized handling of personal information in the private sector. Instead of reviewing the whole spectrum of possible approaches, it focuses on four that are thought to be suitable for the Canadian situation.

The Government has developed a strong role in promoting and adopting microelectronic and communications technology. It therefore has a complementary responsibility to ensure that privacy standards are upheld as the technology is adopted in all sectors of the economy.

The first possible approach would be for government to encourage self-regulation in industries which are important data users. This could take the form of voluntary privacy codes modeled after those used by companies discussed later in this report. The most noteworthy attempts at self regulation also include provisions regarding fair information practices in their customer agreements. Government could work with a representative association in each industry sector in developing a privacy code for that sector. This would produce a series of voluntary privacy codes tailored to fit the requirements of each sector.

A second possibility would be for government to develop legislation which sets out fair information practices and includes a penalty provision for the offense of violating these practices. This could be voluntary in form, covering only those firms which wish to comply, or it could be compulsory, including all important data users in the private sector.

A third possible alternative is to set up a registration and regulation system governing data users. Such a system could set out major principles regarding information handling; set up a Registrar or Commissioner's Office to administer the registration system and ensure compliance with principles; and establish individual rights to access, correction and non-disclosure of personal information. Models of registration systems include the United Kingdom Data Protection Bill as well as systems set up by Canadian provinces to regulate personal credit information.

Combinations of these three approaches would yield other possibilities. One such possibility which is worthy of analysis is a combination of the Self-regulation and Registration approaches described above. For the purposes of this paper, this has been called the "Voluntary Registration" approach. Industry associations could develop privacy codes tailored to their industry, monitor compliance among their members, and mediate complaints from individual citizens. This could be done in consultation with a public Privacy Office which could also keep a registry of all participating associations and companies.

PART I: UNDERSTANDING THE ISSUES

Introduction

The need for informational privacy - the capacity for individuals to determine, in significant measure, what information is collected about them and the manner in which it is made available to others - has long been recognized as a legitimate aspect of a free society. Yet, though the importance of privacy as a value has been widely accepted, its existence has depended in large part on the technological impossibility of detailed surveillance and record-keeping about large numbers of individuals. That technological barrier no longer exists. Therefore, standards will now have to be considered if informational privacy is to be maintained in the face of technological advance.

Key to the creation of such safeguards is the development of a consensus regarding fair information practices. These practices would generally define limits on the way personal information is collected, stored and used. They would also attempt to balance the individual's privacy with competing social values of openness and economic values of efficiency. For the purposes of this paper, personal information may be defined as information in a record about an individual person where that person is identified by name or is readily identifiable by other means.

The purpose of this Discussion Paper is to introduce the reader to the major issues raised by the potential impact of technological developments on individual privacy and to discuss some of the alternative approaches to their resolution.

Recent developments in computer and telecommunications technology have made it possible to process and link information held in a variety of data banks with ease, low cost and speed. In the past quarter century record-keeping by both

government and private entities has moved from the slow, clumsy era of paper files, where information is entered manually, to high speed, efficient, machine-readable files. This development has had a number of significant implications for privacy.

First, machine-readable files are more quickly retrieved and more readily and anonymously updated. What was once a collection of pieces of paper, with the age of each readily apparent, is now a computer readout. Moreover, computer files are easily accessible from many distant points in the organization. More important, however, is the fact that computerized files are readily merged, allowing a number of files dealing with the same subject or individual to be compiled into a single dossier. This can be done within the organization which collected the data. However, data can also be easily transferred to another information user and combined with other files from other sources for uses not envisioned by any of those persons associated with the initial information-gathering process. This is made easier by the use of a single identifying number, but the absence of such a number is not a significant bar to such compilations. In addition, telecommunication links between the holders of files make it possible for the files collected by one institution for one purpose to be shared with other information users for quite different purposes. This process is called data linkage.

The potential impact of efficient retrieval, sharing and merging of files on informational privacy is magnified by the sheer number and variety of sources of computerized information about individuals. The physical size of computers has dropped in twenty years from room-sized machines to ones which fit easily on a desk top. Costs of machinery and processing have dropped at a comparable rate. The older generation of machinery required extensive training to use; present equipment, dubbed "user friendly", can be operated with little specialized training or knowledge.

Where once only the largest institutions, including government, had the resources to effectively use the computer, computerized record keeping is now the norm in virtually every area of human activity. Once the national census was the sole compilation of varied facts about individuals. Now it is possible to compile even more varied information about individuals by the sharing of information among file holders. In government, files held on individuals include information on vital statistics, tax, criminal and court proceedings, health, driving, military and school records, among others.

In the private sector, information held on individuals in computerized files is even more varied. Among the best-known is the credit-rating file. However, the public is becoming aware of other computerized files including those in the insurance, banking and telecommunication industries. In addition, there are many data users of which the public is unaware: retail sellers who have credit card systems or tele-shopping services; magazines which keep subscription lists; charitable, business, professional or community organizations; and many other service providers. As cable television companies enter into two-way operations which make it possible for the consumer to undertake telebanking, teleshopping, and instant polling, and order television programs on a "pay per view" basis, greater amounts of personal data will be stored by the private sector.

This all pervasive collection of personal information is a virtually unavoidable feature of life in the last quarter of the twentieth century. As the U.S. Privacy Protection Study Commission concluded in 1977:

It is now commonplace for an individual to be asked to divulge information about himself for use by unseen strangers who make decisions about him that directly affect his everyday life. Furthermore, because so many of the services offered by organizations are, or have come to be considered, necessities, an individual has little choice but to submit to whatever demands for information about him an organization may make.

Fair Information Practices

This threat to privacy has resulted in a number of attempts to define appropriate limits and to protect the privacy of personal information stored in computer systems. The general principles enunciated in the Council of Europe's "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data" are typical of efforts in a number of jurisdictions to establish guidelines which recognize the benefits of computerized record keeping and the value which individuals place on personal privacy. These guidelines include the following concepts:

- i) Personal information should be obtained and processed fairly and lawfully;
- ii) Personal information should be held for a specified and legitimate purpose or purposes;
- iii) Personal information should not be used or disclosed in a way incompatible with those purposes;
- iv) Personal information should be adequate, relevant, and not excessive in relation to the specified purposes;
- v) Personal information should be accurate and, where necessary, kept up to date;
- vi) Personal information should be kept in name linked form for no longer than is necessary for the specified purposes;
- vii) The data subject should have access to information held about him or her and be entitled to its correction or erasure where the legal provisions safeguarding personal data have not been complied with;
- viii) Appropriate security measures must be taken against unauthorized access, alteration or dissemination, accidental loss and accidental or unauthorized destruction of data.

These guidelines recognize the individual's need to ensure that information which is gathered about him is done so with his consent; that this consent is given with a full and

accurate understanding of the purpose for which the information is gathered; that other uses will not be undertaken without prior consent; that the file will be made available so that the individual can ensure the information is correct; that, in the event there is disagreement about the accuracy of the information, the data subject's version will be noted; and that third parties will not be given access without the individual's knowledge or permission except where required by law.

Even where there is general agreement with these principles in both the public and private sectors, however, there are a number of impediments to their fulfillment. One of these is the companion principle of freedom of information. If an individual has full control over all his personal information, this right can present a major barrier to the rights of others to obtain information on government activities. Clearly a balance must be struck.

Another impediment is the problem of computer crime, where data is taken or released without the permission of the data bank owner. It has been suggested that criminal code amendments which would establish specific offences relating to computer crime would go part way to solving this problem. However, owners of data banks would still have to take reasonable precautions inside their organizations to ensure that personal information is kept confidential and that employees handling this information follow necessary safeguards.

A third potential impediment is the problem of transborder data flow, when information relating to individuals is removed to and processed in another jurisdiction where privacy is not adequately protected by business practices or by law. Here again efficiency and the value of the free flow of information may come into conflict with privacy norms. Certain of these issues are beyond the scope of this discussion since they fall within the realm of the Federal Government.

Public Perceptions

Recent surveys indicate that concerns about privacy brought on by growing computer use are not the sole preserve of academics, futurists, and policy makers. Surveys conducted for the Ontario Government in 1980 and 1983¹ show that a considerable majority of Ontario citizens are concerned about computers affecting personal privacy. In addition, in 1983, about half the population felt that government has the major responsibility for ensuring confidentiality of personal and financial information in our society. An additional 38 percent saw the private sector as having major responsibilities for privacy protection. The earlier 1980 survey further revealed that a sizeable minority believe that institutions such as government, credit-grantors, employers and insurance companies ask individuals for too much personal and financial information.

As well, a 1981 Gallup² survey on attitudes toward microelectronic technology asked respondents to indicate the importance of thirteen issues associated with computers and information technology. Privacy and confidentiality of personal information was by far the most important of the issues and was mentioned by 63 percent of the respondents. The number of people controlling information, a closely related issue, was third in importance, mentioned by 45 percent of respondents. Concern for privacy was highest among those who reported that they had knowledge of microelectronics and among respondents who held executive, sales and clerical jobs. Individuals were also asked to look ahead for the next five years and predict whether or not their privacy would be "invaded or seriously disturbed" by any of seventeen organizations, entities, or

1. See Ontario Consumer Issues 1980 and Ontario Consumer Issues 1983, Ontario Ministry of Consumer and Commercial Relations.

2. A Gallup Survey of Electronic Technology, March 1981, The Gallup Organization, Inc.

persons. There was a high level of concern. Fifty percent or more of the respondents indicated that they believed that each of the following entities could be the source of an invasion of privacy: a credit rating agency, a computer or data bank, an insurance company, the provincial or federal government, a bank, someone who could interfere with their mail, and someone telephoning them. Again, people who reported knowledge of microelectronic technology were those most likely to anticipate the likelihood of a privacy invasion.

A November 1982 survey conducted in London, Ontario by Professor Neil Vidmar of the University of Western Ontario³ for the Ontario Government indicated similarly high levels of concern for privacy in the development of interactive services on cable television. Over two-thirds of those surveyed believe that Canadians have less privacy now than ten years ago. The types of information identified as most sensitive and most in need of protection were bank balances, information on when a person enters or leaves his or her home (information collected by home security systems delivered by cable), credit records, personal earnings and medical records. The findings showed that nearly half of the survey respondents were worried about government use of information, but an even greater proportion distrusted private business. Seventy-two percent of the sample favored regulatory intervention by government, with a majority of 52% seeing a regulatory role for both the federal and provincial governments. The study also indicated a widespread belief that many public and private organizations collect more personal information than is necessary.

3. Neil Vidmar, Privacy and Two-way Cable Television: A Study of Canadian Public Opinion, University of Western Ontario, 1983.

Industry Response

As the OECD guidelines⁴ have noted, one major means to effective privacy protection is the development of self-regulation by industries and firms which make extensive use of personal information. Several firms in this category have responded to the challenge of self-regulation with well-developed internal practices, corresponding to the common definition of fair information practices outlined by the OECD, among others.

Bell Canada, for example, is a major corporation which handles a substantial amount of personal information which is necessarily collected for billing purposes. Company policies consider all subscriber information except name, address and telephone number to be private information held on a need-to-know basis within the company. Personal data are not available for sale, and Bell employees are instructed that all information about customers, wherever collected, is strictly confidential. Indeed the existence, content or nature of any customer communications are not to be made known to third parties, except in compliance with a legal order. Should such an order be made, Bell will notify the customer of the order unless specifically prohibited from doing so.

The Bank of Montreal is another personal data user which has developed and published information on its specific privacy protection practices. Data collected and maintained on file is the minimum necessary for the service desired. Access to that information is strictly controlled within the company, and information is generally not conveyed to third parties without the customer's consent, except that required by stat-

4. Organization for Economic Cooperation and Development, Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data.

ute or court order. Customer applications for credit card services, personal loans and mortgage loans, however, include a general consent or waiver clause which authorizes the bank to disclose information about the customer to third parties under certain circumstances. The practice of requiring customers to sign waivers, common among financial institutions, has been criticized in the past as undermining the customer's privacy protection.

Industry-wide self-regulation through establishment of a privacy code is currently being developed by the cable industry in Canada through its association, the Canadian Cable Television Association. A CCTA sub-committee, using the highly regarded Warner-Amex cable privacy code in the United States as a starting point, is in the process of creating a code for the industry tailored to the Canadian situation. It is expected that this code will be accepted and implemented by CCTA member companies as they develop their interactive service offerings. A major advantage of code development prior to the development of services is that systems can be designed in advance to enhance computer security and data protection capabilities.

Companies with voluntary privacy codes are still the exception rather than the norm, however. It is clear, therefore, that the widespread computerized handling of personal information will require the setting of standards in some form to ensure that infringement of citizens' privacy rights do not occur.

PART II: LEGISLATION GOVERNING PUBLIC SECTOR DATA BANKS

There is a growing body of legislation, in Canada and abroad, which addresses itself to the issues surrounding information access and privacy. That most of it is of fairly recent origin reveals the extent to which these issues are interconnected with developing information technologies and the speed with which privacy problems are expected to reach serious proportions. A variety of solutions are in evidence here, some dealing only with the question of privacy as affected by government data banks, others addressing the question of private sector data protection as well.

Canada

Privacy protection on the national level in Canada is focused on development of fair information practices in government data banks under federal jurisdiction. The Canadian Privacy Act, passed in 1982 and proclaimed in 1983, establishes the right of Canadian citizens and permanent residents to know, with certain exceptions, of the existence of information files on them; to examine, correct and challenge information in them; to know to what uses the file has been put; and to be consulted regarding certain future uses thereof. A companion statute, the Access to Information Act, was designed to maximize compatibility between information access and privacy. The Privacy Act requires publication of an annual index to federal information banks, and creates a Privacy Commissioner with the power to mediate disputes, investigate to ensure compliance by the data bank holder in question, and apply to the courts for review of government decisions to withhold information.

Provinces

Both Nova Scotia and New Brunswick have freedom of information legislation dating from the late 1970's. Nova Scotia's lists the types of documents that may be accessed, rather than establishing a general access principle, while the New Brunswick Act establishes general principles, with appeals to an ombudsman and in camera inspection by the courts of contested documents.

Newfoundland passed both Freedom of Information and Privacy Acts in 1981. The former lists the departments, boards, agencies and commissions affected, while the latter makes it "a tort, actionable without proof of damage, for a person...to violate the privacy of an individual."

Quebec deals with freedom of information and privacy together in an Act passed in 1982 and designed, like the federal Act, to protect personal information in government files, while allowing access to documents of public bodies. These bodies include not only the provincial government and all its departments and agencies, but also municipalities (including county, regional and city governments and agencies), and educational, health and social service institutions. The Act requires that an index of files kept by public bodies be compiled for circulation by The Information Access Commission and that requests for information be processed free of charge and within twenty days of receipt. The Commission has a variety of supervisory, investigatory and decision-making powers.

Ontario has examined the questions of privacy and access to information extensively in the past. As a result it has been proposed, in Ontario's Privacy and Access to Information Bill, that fair information practices be defined and made obligatory for government data banks. The proposal would establish a Data Protection Office with authority to develop and apply standards for the management of personal data systems. These standards would include requirements to restrict

information collection to the minimum essential for the operation of a program; provide that personal information normally be collected directly from its subject, and that the reason for its collection be disclosed; and generally require that information collected not be disclosed without the individual's consent. Exceptions to the rule of authorized disclosure include occasions where it would not represent an unwarranted invasion of personal privacy, where it is necessary for the administration of authorized government programs, or where it is in the best interests of the individual or society. Individuals would also have the right to access and correction of files, with the data holder obligated to notify past users of the file of any correction. Individuals would also have the right to file complaints to a separate Commissioner's office.

In 1968 British Columbia passed The Privacy Act and became the first Commonwealth jurisdiction to establish an independent cause of action for the unreasonable and unwarranted invasion of an individual's privacy. This Act was followed by similar legislation in Manitoba and Saskatchewan. None of these privacy Acts, however, deal expressly with the inappropriate or unauthorized use of personal information which has been given voluntarily to another person or institution and integrated into an information bank. Moreover, there is a strong financial disincentive to the individual in enforcing his or her rights through the courts, since the costs of the action would often outweigh potential benefits.

United States

The United States' Privacy Act dates from 1974 and applies to personal information held in government records. It is essentially a "good housekeeping" statute which sets standards for administration of data files. As such, it requires government to report regarding the existence of information files, to ensure the quality of the information therein, to provide access to the subjects of such files, to use data only

for the purposes for which it was collected, and to provide a record of disclosures of that information to the individual affected. There are no time limits for response, and the Act is self-enforcing in that the individual affected has recourse to the courts rather than a separate authority. The United States also has a Freedom of Information Act with rather wider rights of access than the Privacy Act.

United Kingdom

Parliament is now in the process of considering data protection legislation which encompasses both private and public sector automated data banks. It establishes a Data Protection Registrar and Tribunal; requires that both private and public data banks be registered (with certain exceptions); prohibits unauthorized disclosure of information; provides access for individuals to data in registered data banks; and entitles them to amend files and to seek compensation in the courts for damages suffered. The Registrar is empowered to de-register data banks which contravene data protection principles and can prohibit the transfer of data outside the United Kingdom where the country of destination fails to meet minimum data protection standards. This legislation will enable the United Kingdom to adhere to the Council of Europe Convention on data protection.

Federal Republic of Germany

While there is no general access to information law, the Federal Republic of Germany has a highly developed network of data protection arrangements aimed at safeguarding personal privacy. These include both the Federal Data Protection Act and state data protection legislation, which enshrine in law the data protection principles of the Council of Europe. The Federal Act covers both federal public sector data banks and the private sector on a nationwide basis, while state Acts

each govern their respective government's data practices. Primary responsibility for ensuring that the laws are followed falls on the heads of government agencies which create and use personal information files. As well, both Federal and state legislation provide for the establishment of the office of Data Protection Commissioner, with responsibility to supervise and advise agencies which handle personal data and to report to the legislature annually. The success of this system of data protection lies not in the coercive powers available to the Data Commission, but on the high degree of consciousness of appropriate data handling procedures which has been achieved both in the public and in government.

Sweden

Sweden has been the world leader in both access to information and data protection legislation. Access to government information is regulated by the Freedom of the Press Act and the Secrecy Act, which taken together, provide access within a set of specific and limited exceptions. Information privacy is provided through several legislative Acts, the most important of which is the Data Act of 1973. This Act created a Data Inspection Board to regulate the collection and use of personal data in computerized form in both the public and private sectors. Thus the major function of the Board is the licensing of all data registers held by government or private sector data users, and the setting of the rules which govern their use. Decisions of the Board can be appealed to the Minister of Justice and to Cabinet, though the number of such appeals has consistently been small. In general, the first priority of the system is the protection of personal privacy, with less weight given to economy and efficiency in data use.

Council of Europe

The Council of Europe has prepared a "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data" which has as its purpose the securing of respect for the individual's right to informational privacy. It requires signatory states to give effect in domestic law to the basic principles for data protection embodied in the Convention. These include: fair information gathering practices; limitations on use and contents of files in light of the purposes for which they were gathered; accuracy; minimal identification of individuals; limitations on the kinds of data to be processed; appropriate security measures; and procedures for identification, examination and correction of files by the individual to whom they pertain. It also confirms the right of signatory states to refuse to allow personal information to be sent to countries without comparable data protection provisions.

Organization for Economic Cooperation and Development (OECD)

The Council of the OECD has developed guidelines governing the protection of privacy, which it regards as minimum standards for its members. In a manner similar to the Convention of the Council of Europe, the OECD subscribes to the following principles: collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation and accountability. While specifically noting that data protection should not provide an excuse for restriction of transborder data flow, the OECD agrees that member countries should prevent the export of data which circumvents domestic privacy legislation, or involves export of data to countries not substantially observing the OECD principles. In particular, member countries are urged to: adopt appropriate domestic legislation; encourage and support self-regulation; provide reasonable means for individuals to exercise their rights; provide adequate sanctions;

and ensure that there is no unfair discrimination against data subjects.

Summary

The preceding discussion suggests that the privacy legislation in these various jurisdictions covers a wide spectrum. Most laws ascribe to a similar set of fair information practices or principles. Although there is some variation on finer points, such as whether or not information collected must be "relevant" and collected "directly", most laws establish individual rights to access and correction, and build in some controls over the transfer of personal information to third parties. However, beyond this basic similarity, these laws vary greatly in their strength and application.

For the purposes of this paper, it is worth noting three of the models discussed above. The United States Privacy Act, at one end of the spectrum, provides an example of a self-enforcing law which sets out certain individual rights but does not establish a separate enforcement agency. The Act leaves it up to the individual to seek recourse through the courts.

A second model, illustrated by the Canadian Privacy Act, establishes an enforcement agency with investigation and monitoring responsibilities. Aggrieved individuals can complain to the Privacy Commissioner who can also apply to the courts for review of government decisions to withhold information. The new Quebec law has some similarities, although it has wider application, covering municipalities, school boards, universities and health and social service agencies as well as government departments. The Quebec law gives its Commission significant powers to supervise information practices, respond to complaints, conduct investigations, and issue binding orders to a public body.

A third model that could be identified on this spectrum is illustrated by the United Kingdom registration system described above. In some ways this system of regulation is stronger than the two models summarized above because it requires the formal registration of data banks and gives the Registrar substantial powers of investigation and enforcement, including the power to refuse registration of data banks if the user does not comply with the principles of the Act. The Swedish and German registration systems go further and could be regarded as two additional models on this spectrum.

PART III: ALTERNATIVES FOR THE PRIVATE SECTOR

Summary of Issues

The first part of this paper has discussed the challenge which computerized handling of personal information poses for the protection of privacy. From this discussion emerge a number of competing notions. Most would agree that there is a need to weigh the gains in computer efficiency and speed against the costs to individual privacy which have arisen. In economic terms, therefore, there are conflicting pressures for business establishments to achieve all the cost savings new technology has to offer on the one hand, and to provide the individual with reasonable privacy protection, on the other.

Although it is difficult to generalize, the cost of providing minimum privacy protection is thought not to be great in relation to the efficiency savings usually afforded by new technology. Moreover, these "protection" costs are often minimized if standards or procedures are established prior to the introduction of new systems.

The privacy issues outlined in Part I could be summarized as follows:

- 1) Data Collection: Should personal information collected by data users⁵ be limited to that which is relevant to the user's specified purpose and to that which has received the data subject's informed consent? Should there be a further requirement that personal information be

5. The following definitions are used in this section:
Date User: Institution which collects and handles personal information on individuals.
Data Subject: Individual who is the subject of data collection.

collected directly from the data subject? The major statements of principle on the data collection issue usually also include a reference to data being obtained fairly and lawfully for a legitimate purpose. This paper assumes that legitimacy is not at issue and will focus on relevance and informed consent with regard to data collection.

- 2) Data Quality: Should personal information collected by data users be subject to a requirement to be accurate, complete and up-to-date?
- 3) Disclosure Limitations: Should disclosure of personal information by data users to third parties be limited to only that information required to fulfill the user's specified purpose? Exceptions would include cases where the subject consents or where disclosure is compelled by law.
- 4) Security Safeguards: Should data users be subject to a requirement to ensure the physical security of personal records?
- 5) Individual Access: Should data subjects have the right to confirm the existence of their personal data in records, inspect and receive copies of the data, and request changes to erroneous or incomplete data?
- 6) Costs: If citizens are given rights of access, correction and non-disclosure, the cost of enforcing these rights must not be prohibitive. Regulatory options which give enforcement agencies quasi-judicial powers to settle grievances may present one option for providing enforceable rights for individuals.

This section will analyze a number of alternative solutions to these issues as they apply to the private sector and then review the strengths and weaknesses of each alternative. The analysis begins with the assumption that the need for informational privacy is a legitimate claim and that the principles enunciated by the Council of Europe's Convention on Data Protection (summarized on page 4) represent a reasonable list with which to evaluate policy alternatives in this area.

Scope

This paper attempts to deal with both the public and private sectors. From the individual citizen's point of view, the threat to privacy of personal information exists in both sectors. Although North American privacy laws have thus far only addressed the problem in the public sector, countries like the United Kingdom⁶, West Germany and Sweden have legislative programs in place which cover both sectors.

This leads to the question of self-regulation or government regulation. Some of the competing arguments concerning the effectiveness and desirability of self-regulation as a means of ensuring fair information practices will be examined below in the context of the private sector.

Another general question which all jurisdictions have to decide is whether regulatory programs should cover only computerized personal records or whether they should apply to all personal records, manual and computerized. The major premise in the United Kingdom's White Paper⁷ on data protection is that computerization presents new threats to privacy because

6. At the time this report was written the U.K. Bill had passed Second Reading.

7. Data Protection: The Government's Proposals for Legislation, Home Office, United Kingdom, April 1982.

of the speed, low cost and ease with which personal information can now be distributed. The implication here is that the costs and effort involved in the transferring of information in manual files act as a disincentive to unauthorized disclosure.

On the other hand, the data protection laws covering public sector records in North American jurisdictions do not distinguish between computerized and manual records. These laws provide the individual with certain rights regarding personal information in both computerized and manual records. The importance of manual records is seen when categories such as health information are considered.

Another important question is whether all data banks, or only those above a threshold size, should be covered by whatever regulatory or self-regulatory approach is undertaken. It is argued by some that only those data users above a threshold size should be candidates for regulation, since the cost of compliance is a greater burden for smaller institutions. However, exemption of smaller data banks would leave information in those banks unprotected, thereby weakening individual rights.

Policy Options

This section looks at four possible options: a voluntary privacy code, a legislated code, a registration and regulation system, as well as an approach which combines elements of the first three. This list is not intended to be exhaustive, but to offer for discussion some reasonable alternatives which could fit the Canadian situation.

1) Voluntary Privacy Code: If the need for privacy protection is accepted as a legitimate claim, governments could encourage specific industries (through their associations) and corporations which are important data users to develop

voluntary codes, incorporating the important principles normally embodied in data protection laws. Companies such as Warner-Amex in the U.S. and IBM in Europe have already developed guidelines for the protection of personal information in their files. In Canada, the Canadian Cable Television Association is in the process of developing a privacy code.

In 1981, Warner-Amex Cable Communications Inc. developed a code designed to protect the privacy of personal information which the company compiles on individual subscribers of cable TV services. In the code, the Company agrees to keep subscriber information physically secure and confidential and agrees to keep subscribers informed of all information gathering functions of the cable TV services being provided. Agreements with individual subscribers set out the terms under which information will be used and provide that no other individual data will be collected without the individual's consent. The code also gives the subscriber the right to examine his or her file and request corrections of erroneous data.

The code is being made a part of subscriber contracts and franchise agreements, making it self-enforcing and giving the subscriber certain rights by agreement. In theory, an individual who felt that his privacy rights had been infringed could commence a civil legal action for breach of contract.

Comments: The advantages and disadvantages of the voluntary code approach as a resolution to privacy issues could be summarized as follows:

- . It provides no assurance that the majority of important data users will voluntarily adopt codes.
- . No formal enforcement or compliance methods are established (except the limited power of the individual to seek recourse for breach of contract, in cases where the code is supplemented by a written agreement between data user and subject).

- . It imposes the least cost and interference on data users.
- . It features maximum flexibility, since codes could adapt to changing technology and public requirements.
- . It does not guarantee substantial rights for individuals in the case of a dispute over access, correction or disclosure.
- . The adoption of various voluntary codes by different industry sectors and companies would result in a lack of uniformity of privacy protection for individuals.

2) Legislated Privacy Code: One approach which falls in between voluntary codes and more traditional government regulatory solutions, consists of developing legislation which would set out fair information practices and would include a penalty provision for the offense of violating these practices. Fair information practices could cover the issues of data collection and quality, disclosure limitations, security safeguards and individual access as set out above. This law would permit a civil lawsuit in tort and would essentially constitute a self-regulatory approach to the problem since it would not require the establishment of an enforcement agency.

Some authors have suggested that public demands for privacy rights have arisen from the failure of legislatures and courts to develop such a body of law⁸. It is generally agreed that the common law in Commonwealth countries offers no protection for personal privacy per se.

8. For example, see Roger Noll, "Regulation and Computer Services", in M. Dertouzos and J. Moses, The Computer Age: A Twenty-Year Review, (Cambridge: MIT Press, 1980) and Murray Rankin, Privacy and Technology: A Canadian Perspective (Canadian Institute for Legal Studies, Cambridge University, 1983).

The Privacy Acts enacted by British Columbia, Saskatchewan and Manitoba have been used infrequently and are also thought not to provide the individual with substantial remedies for the types of privacy problems brought on by the computerized handling of personal information.

Legislation establishing a privacy code could take one of two forms:

- (a) An Act could permit voluntary compliance. Regulations to the Act could register those industries or companies which wish to comply. Voluntary participants would thus be identified as privacy-conscious companies in their field.
- (b) Alternatively, an Act could require compliance. It could apply to all data users, or only to those institutions with data banks above a threshold size.

Comments: Following is a summary of the strengths and weaknesses of this approach:

- . It provides no assurance that a majority of data users would voluntarily comply. Only the compulsory version of such a statute would guarantee participation by a majority of data users.
- . The remedy available to the individual is costly and impractical. It would likely not be used often since the cost to the individual would almost always exceed possible benefits from using this remedy. Therefore, this approach also does not provide substantial rights to individuals regarding access, correction, disclosure and resolution of disputes.
- . It imposes little cost and interference on data users.
- . It allows a high degree of flexibility, since the legislation would phrase fair information practices

in general terms, thereby not hampering the application of new technology.

- . If remedies were not used widely by individuals, such an Act would not have a major effect on information practices. The compulsory version of such an Act, however, might encourage some uniformity in general data collection and disclosure practices.

3. Registration and Regulation: Another possible solution to these issues is for government to legislate to require registration of data banks; give individuals defined rights of access and correction; regulate the collection and third-party disclosure of personal information; guarantee the security of data and establish a Registrar with investigation and enforcement responsibilities. The registration requirement could apply to those institutions which automatically process personal information in data banks.

This is basically the approach taken by the United Kingdom in their Data Protection Bill, referred to in Part II of this paper. This Bill sets out a registration and enforcement system covering data users which process personal information automatically. Although it applies to both the public and private sectors, the basic structure of this registration system can serve as a useful model for our discussion purposes here.

In this model, the public registry of data users helps individuals become aware of the existence and purpose of computerized personal information banks. The data user is required to identify himself, the information he uses, where it has come from and to whom it is disclosed, as well as the purposes for which it is used. The Registrar has the power to make inquiries, to inspect data files and to require modifications to a system. In extreme cases, he may refuse registration for non-compliance with the major data protection principles embodied in the Act. Since the Registrar is given such

wide powers, the Bill sets up an appeal process to an independent tribunal, composed of judicial and computer experts.

The United Kingdom Bill also gives the individual rights of access to personal data; the right to compensation for damages from use of inaccurate data, loss of data and unauthorized disclosure; as well as the right to apply to the courts for rectification or erasure of incorrect data. The individual would have to apply to the court if a data user contravenes any of these individual rights, in order to secure compliance or seek damages in civil proceedings.

Other features of the Bill enable the Government to restrict the transfer of categories of information to specified countries which do not have data protection legislation of comparable strength; give the power to make regulations governing particular categories of personal data such as racial origin, political and religious beliefs; and exempt the collection of data for research purposes where individuals are not identifiable.

The following comments focus only on the general characteristics of a registration system such as the one modeled in the United Kingdom Bill as they could apply to the private sector. They are not meant as an evaluation of the Bill overall.

Comments: The advantages and disadvantages of this approach could be summarized as follows:

- . It provides legislated privacy protection covering all important data users and includes an enforcement mechanism to ensure compliance.
- . It provides the individual with legal rights of access and correction as well as protection against disclosure to third parties. However, the enforcement of these rights in the case of a dispute may be

costly to the individual since the remedy involves application to the courts.

- . This approach imposes new regulation on the private sector, resulting in additional costs for data users.
- . It allows some flexibility, since the data protection principles are general and the Registrar's powers are defined broadly, allowing him to handle demands of changing technology and information practices.
- . It would have a major impact on information practices because of the registration and enforcement powers.

Registration schemes are a common feature of data protection legislation in other European countries. Brief descriptions of the legislation in West Germany and Sweden, probably the other two most noteworthy examples, are given in Part II.

The major disadvantage of this model from the citizen's point of view is the cost of enforcing his rights through the courts. An alternative model of a registration system could build in the possibility of an appeal from the citizen to a registrar or commissioner who would have the power to issue binding orders affecting the data user. This would remove the cost disincentive for the individual.

Many Canadian provinces regulate the collection and disclosure of personal credit information through credit reporting Acts. In Ontario, for example, the Consumer Reporting Act registers credit bureaus, regulates the gathering, storage and disclosure of credit information, and gives the individual access to his or her personal credit file. The Registrar has the power to revoke or refuse registration under certain circumstances, in which case the applicant is entitled to an appeal to a tribunal. The models used by provinces to regulate

credit information might also provide some guidance to registration systems contemplated for personal data users.

4. Voluntary Registration: Combinations of the above three approaches could produce other possibilities. One such possibility which is worthy of analysis is a combination of the Self-Regulation and Registration approaches described above. Industry associations could develop privacy codes tailored to their industry, monitor compliance among their members, and mediate complaints from individual citizens. This could be done in consultation with a public Privacy Office which could also keep a registry of all participating associations and companies.

Comments: Following is a summary of the strengths and weaknesses of this approach:

- . As in the self-regulation model, this solution offers no assurance that the majority of data users will voluntarily join a registration system.
- . It would establish a monitoring system to encourage compliance by participating companies and agencies. Although this could be a very positive force, no formal compliance or enforcement powers would be available.
- . It would result in some extra costs to data users.
- . It features a great degree of flexibility allowing industry and the coordinating agency to respond to changing technology and information practices.
- . It does not guarantee concrete rights for individuals in the case of a dispute over access, correction or disclosure. The complaint handling activities of industry associations, however, could fulfill a mediation role.
- . Although the adoption of different privacy codes by different industry sectors would result in some differences in privacy standards across the economy,

the coordinating agency could work for uniformity on important issues such as the individual's rights to access, correction and non-disclosure.

Summary

This section has attempted to compare the effectiveness of several alternative methods of resolving informational privacy issues in the private sector. Rather than reviewing all the possible approaches, including more stringent government registration and licencing schemes, this paper has focused on those approaches which are thought to be more suitable to the Canadian situation.

The table on the following page contains a comparative summary of the four approaches outlined above. The criteria used for comparison are based on the preceding analysis and reflect the major consideration central to any discussion of regulatory options: the balance between cost to industry and the provision of individual rights or protections to citizens. Terms in the table, such as "Low/Medium/High" are used to suggest relative values only.

EVALUATION OF ALTERNATIVE SOLUTIONS

A L T E R N A T I V E S

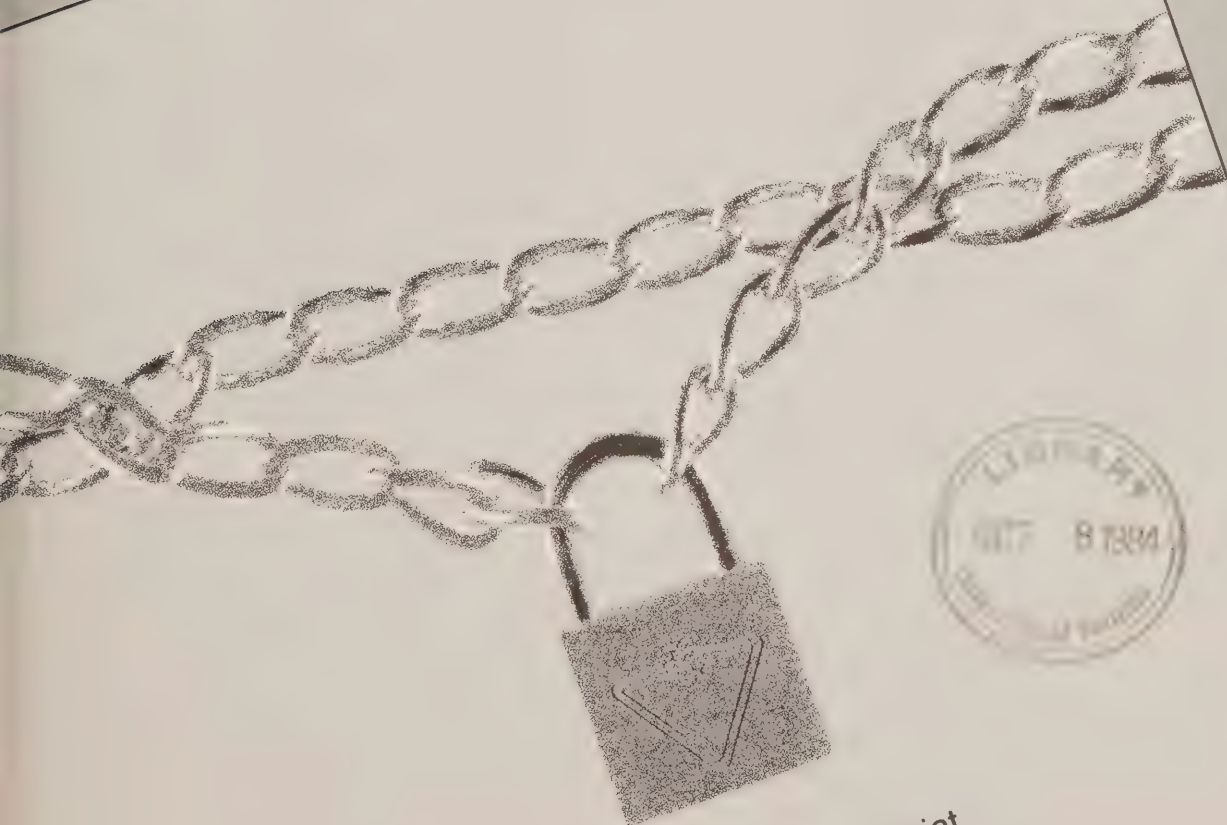
BASIC CRITERIA	VOLUNTARY PRIVACY CODES	LEGISLATED PRIVACY CODES	REGISTRATION AND REGULATION	VOLUNTARY REGISTRATION
Cost of Compliance to Data User	Minimum	Minimum	Moderate to High	Moderate
Flexibility	Maximum	Moderate	Moderate	Maximum
Individual Rights to Access, Correc- tion and Non- Disclosure	No Guarantee	Legislated rights under compulsory version of such a law	Establishes Legal Rights for Individuals	No Guarantee
Individual Rights in Dispute Resolution	None	Costly and difficult for individual to enforce	Costly for Individual to Enforce (Alternative registration systems could remove cost burden on individuals)	None
Uniformity of Information Practices	Difficult to Achieve	Possible under compulsory version of such a law	Registration Encourages Uniformity	Some Uniformity Possible
Effectiveness in Developing Overall Standards for Privacy	Low to Medium	Low to Medium	High Potential	Medium

CA1
Z4
-C52

870-123/004

Government
Publications

Document de travail sur la vie privée projets pour 1984



Ontario

Secrétariat
de la province
au Développement
des Ressources

L'honorable
Norman W. Sterling, c.r.
Secrétaire de la province



Secrétaire
provincial au
Développement
des ressources

Édifice Whitney
Queen's Park
Toronto (Ontario)
M7A 1A2
416/965-7721

MESSAGE DU MINISTRE :

Au cours de la dernière décennie, la protection de la vie privée a posé un problème majeur aux sociétés industrielle modernes. L'inquiétude est allée croissant à mesure que les citoyens se rendaient compte que le bouleversement technologique était tel qu'ils ne pouvaient compter sur leurs seuls efforts pour protéger les renseignements personnels les concernant.

La protection de notre vie privée est un droit auquel nous tenons tous et qui doit être respecté à tout prix. Aussi étrange que cela puisse paraître, ce droit n'a jamais été reconnu officiellement au Canada.

On trouvera dans ce document de travail un choix de propositions que les gouvernements qui cherchent une solution à ce problème pourront examiner. Il est également important que ces questions fassent l'objet d'une consultation avec le secteur privé.

Il est d'autant plus nécessaire, en effet, de répondre de façon uniforme aux préoccupations que suscite cette question que l'on prend davantage conscience du fait que les données recueillies sur un particulier peuvent être conservées et, en fait, utilisées dans une autre province ou un autre pays.

Dans le secteur privé, certaines compagnies ont réagi en soumettant la manipulation des renseignements personnels à des codes visant à protéger leur caractère confidentiel. Les compagnies qui utilisent ce type de code sont cependant davantage l'exception que la règle et il semble qu'il soit nécessaire d'établir des normes pour empêcher toute ingérence dans le droit des citoyens à la protection de leur vie privée.

De nombreux pays d'Europe ont mis en place des lois sur la protection des données personnelles et, en 1981, le Conseil de l'Europe a adopté une convention de protection des données signée par tous les pays participants.

Les inquiétudes suscitées par le droit à la protection des renseignements sur ordinateurs sont très réelles et il est essentiel d'aborder le problème de façon responsable, en collaboration avec l'industrie. J'espère que ce document de travail constituera un premier pas important vers l'élaboration d'un code de protection de la vie privée des citoyens.

Le Secrétaire provincial
au Développement des ressources

Norman Sterling, c.r.

TABLE DES MATIÈRES

	Page
Synopsis	iii
 PARTIE I : COMPRENDRE LES PROBLÈMES	 1
Introduction	1
Pratiques loyales en matière d'information	4
Perceptions du public	7
Réponse du secteur privé	9
 PARTIE II : LOIS RÉGISSANT LES BANQUES DE DONNÉES DU SECTEUR PUBLIC	 11
Canada	11
Provinces	12
États-Unis	14
Royaume-Uni	14
République fédérale de l'Allemagne occidentale	15
Suède	16
Conseil de l'Europe	16
Organisation pour la coopération et le développement économique	17
Résumé	17
 PARTIE III : SOLUTIONS POSSIBLES POUR LE SECTEUR PRIVÉ	 20
Résumé des problèmes	20
Portée du document	22
Politiques possibles	24
Résumé	32

SYNOPSIS

Les progrès de la technologie des ordinateurs et des télécommunications ont soulevé des questions nouvelles sur la protection des renseignements personnels - c'est-à-dire le droit qu'ont les particuliers de savoir quelles informations sont recueillies à leur sujet et la façon dont elles sont communiquées à des tiers. Ce document de travail passe en revue un certain nombre de graves problèmes que risque de poser l'impact de l'évolution technologique sur la protection de la vie privée et examine divers moyens de les résoudre.

Les problèmes présentés portent sur la protection des données, la qualité des données, les limites de la divulgation, la défense de la sécurité, les coûts et l'accès individuel aux fichiers de renseignements personnels dans les banques de données informatisées. De récents sondages de l'attitude du public semblent indiquer que les particuliers sont très préoccupés par les effets de l'ordinateur sur leur vie privée et par les institutions qui recueillent trop de renseignements personnels à leur sujet.

Le secteur public a commencé à aborder ces problèmes par le biais de divers textes de loi qui définissent, pour les banques de renseignements des ministères et organismes gouvernementaux, les pratiques loyales en matière d'information et prévoient comment les appliquer. On peut citer, à titre d'exemple, la Loi fédérale sur la protection des renseignements personnels et le Bill 65 du Québec, assortis l'un et l'autre de bureaux mis en place pour veiller au respect des normes établies dans ce domaine et étudier les plaintes individuelles pour pratiques déloyales en matière d'information.

En Ontario, un projet de loi est à l'étude. Il s'agit du Privacy and Access to Information Bill, qui vise à imposer aux banques de données du gouvernement provincial des pratiques loyales en matière d'information. La loi serait accompagnée d'un bureau chargé de la faire appliquer et d'un autre qui serait habilité à recevoir les plaintes des citoyens en la matière.

En Europe, la protection des données est à l'ordre du jour et des pays comme le Royaume-Uni, l'Allemagne de l'Ouest et la Suède ont des programmes législatifs qui prévoient l'enregistrement des fichiers de données et régissent les pratiques en matière d'information dans les secteurs public et privé.

Le secteur privé, conscient du problème, a mis au point des méthodes internes et, dans certains cas, des codes volontaires visant à protéger les renseignements personnels suivant certains principes courants dans la législation sur le sujet. Aux États-Unis, Warner-Amex Cable Communications Inc. a mis au point un code qui protège le caractère confidentiel des données recueillies sur ses clients.

L'Association canadienne de télédistribution est en train d'élaborer un code de protection visant une auto-réglementation similaire.

Dans le passé, ce sont les bureaux de crédit, assujettis dans la plupart des provinces à des lois sur la divulgation des données relatives au crédit, qui ont été les principaux manipulateurs de renseignements personnels dans le secteur privé. On enregistre cependant un accroissement des fichiers informatisés de renseignements personnels dans toutes sortes de secteurs, notamment les institutions financières, les services de télédistribution, les services vidéotex, les services informatiques, ainsi qu'une multitude d'autres secteurs commerciaux et non commerciaux. Le particulier n'a pas de garantie concrète contre l'ingérence dans ces fichiers.

Si elles veulent aborder le problème de la protection de la vie privée de façon uniforme, les diverses instances canadiennes vont se heurter à un certain nombre de questions légales. À qui appartiennent les données personnelles contenues dans les fichiers? Comment peuvent-elles être légalement protégées? Les lois en vigueur sur la protection des données personnelles doivent-elles être amendées en fonction de l'évolution technologique? Qui est responsable de la divulgation impropre ou non autorisée de renseignements personnels? Et puis, bien sûr, il faudra faire face à l'éternel problème du partage des compétences entre les gouvernements fédéral, provinciaux et territoriaux, si l'on veut harmoniser les règlements à mesure qu'ils sont édictés et éviter les conflits entre les lois.

On estime généralement que les droits individuels, y compris les droits à la protection de la vie privée, ne relèvent de la compétence législative exclusive ni du gouvernement fédéral ni des gouvernements provinciaux, mais sont plutôt déterminés par la Constitution canadienne, et plus particulièrement par les articles 91 et 92 de l'Acte de l'Amérique du Nord britannique. Bien qu'un certain nombre de gouvernements aient déjà des lois sur la question, il est important que ces initiatives se poursuivent et, peut-être, s'amplifient.

Ce document de travail analyse quatre méthodes de résolution des problèmes que pose, pour la vie privée des citoyens, l'accroissement de la manipulation informatisée des données personnelles dans le secteur privé. Au lieu de passer en revue la gamme entière des mesures possibles, il en privilégie trois qu'il estime correspondre à la situation canadienne.

Le gouvernement a joué un rôle important dans la promotion et l'adoption de la technologie de la microélectronique et des communications. Maintenant que la technologie est acceptée dans tous les secteurs de l'économie, il lui incombe d'accorder son soutien à l'établissement de normes de protection de la vie privée.

La première approche possible consisterait, pour le gouvernement, à encourager l'auto-réglementation dans les industries qui font une utilisation importante de données. Cela pourrait prendre la forme de codes volontaires sur le modèle de ceux qu'utilisent certaines compagnies dont on parlera plus loin. Les tentatives d'auto-réglementation les plus dignes d'intérêt contiennent également des dispositions sur les pratiques loyales en matière d'information dans les contrats avec les clients. Le gouvernement pourrait travailler, de concert avec une association représentative de chaque secteur industriel, à mettre au point un code de respect de la vie privée correspondant à ce secteur. Cela produirait une série de codes volontaires conçus en fonction des exigences de chaque secteur.

Deuxièmement, le gouvernement pourrait aussi édicter des lois qui définissent les pratiques loyales en matière d'information et prévoient une pénalité en cas d'infraction. L'application de la loi pourrait être volontaire et ne concerner que les établissements qui choisissent de s'y conformer, ou obligatoire pour tous les secteurs qui font un usage important de données.

Une troisième méthode consisterait à établir un système d'enregistrement et de réglementation auquel seraient assujettis les utilisateurs de données. Ce système pourrait définir les principes majeurs de manipulation de l'information; instituer un registraire ou un commissariat pour administrer le système d'enregistrement et veiller à ce que les principes soient respectés; et établir le droit des particuliers touchant l'accès, la correction et la non-divulgaration des données personnelles. On trouve des modèles de systèmes d'enregistrement dans la loi sur la protection des données (Data Protection Bill) du Royaume-Uni et dans les organes mis en place par les provinces canadiennes pour réglementer les renseignements personnels en matière de crédit.

Enfin, la combinaison de ces trois façons de procéder fournirait d'autres possibilités dont une qui mérite l'attention, à savoir une combinaison des systèmes d'auto-réglementation et d'enregistrement décrits ci-dessus. Aux fins de ce document, on a donné à cette méthode le nom d'"enregistrement volontaire". Les associations professionnelles pourraient élaborer des codes correspondant à leur secteur, veiller à ce que leurs membres s'y conforment et se faire les médiateurs des plaintes des particuliers. Ceci pourrait se faire en consultation avec un commissariat public à la protection de la vie privée qui tiendrait également un registre de toutes les associations et compagnies participantes.

PARTIE I : COMPRENDRE LES PROBLÈMES

Introduction

Il y a longtemps que le droit de l'individu à la protection de ses données personnelles et de sa vie privée - c'est-à-dire le pouvoir qu'il a de déterminer en grande mesure quels renseignements sont recueillis à son sujet et de quelle manière ils peuvent être utilisés par des tiers - constitue un aspect légitime d'une société libre. Or, bien que l'importance du respect de la vie privée soit généralement reconnue, son application dépendait en grande partie de l'impossibilité technologique où l'on se trouvait de procéder à une surveillance étendue et de tenir des dossiers détaillés sur un grand nombre d'individus. Cette barrière technologique n'existe plus. Il faut donc envisager d'établir des normes, si l'on veut que les données personnelles soient protégées dans le cadre du progrès technologique.

Pour prendre de telles mesures de sécurité, il est essentiel de s'accorder sur la définition de ce qu'on appellera des pratiques loyales en matière d'information. Ces pratiques fixeraient des limites générales à la façon dont les renseignements personnels sont recueillis, conservés et utilisés. Elles chercheraient aussi à équilibrer le droit de l'individu à la protection de sa vie privée avec les valeurs sociales et économiques également importantes d'ouverture et d'efficacité. Aux fins de ce document, on entendra par données personnelles les fichiers de renseignements sur une personne dans lesquels elle est identifiée par son nom ou facilement identifiable par d'autres moyens.

Le but de ce document de travail est de sensibiliser le lecteur aux problèmes majeurs que soulève l'impact possible de l'évolution technologique sur le droit des personnes à la protection de leur vie privée et de discuter des solutions possibles à leur apporter.

Les dernières innovations technologiques en matière d'ordinateurs et de télécommunications permettent de traiter et de relier des informations conservées dans diverses banques de données facilement, rapidement, et à bas prix. Au cours des vingt-cinq dernières années, la tenue des dossiers dans le secteur public et le secteur privé est passé de l'âge de la paperasse lente et encombrante, où les renseignements sont enregistrés à la main, au système de fichiers éclairs efficaces et lisibles par une machine. Cette évolution a eu un certain nombre de conséquences notables sur la vie privée des individus.

Tout d'abord, l'extraction de dossiers lisibles par une machine se fait plus rapidement et la mise à jour est plus facile et plus anonyme. Ce qui était autrefois un ensemble de documents dont la date était clairement apparente est devenu écran d'ordinateur. De plus, les dossiers informatisés sont facilement accessibles en des lieux éloignés de l'organisme. Ce qui est encore plus important, cependant, c'est qu'on peut facilement fusionner les dossiers informatisés, ce qui permet d'assembler dans un seul fichier un certain nombre de pièces traitant du même sujet ou de la même personne. Cela peut se faire au sein de l'organisme qui a recueilli les données, mais ces dernières peuvent également être transmises sans difficulté à un autre utilisateur d'informations et combinées avec d'autres dossiers en provenance d'autres sources, à des fins non prévues par les personnes touchées par le processus initial de collecte de l'information. Ceci est plus facile à accomplir si l'on a un numéro d'identification, mais le manque de numéro n'est pas un obstacle suffisant pour empêcher ce type de compilation. En outre, le réseau de télécommunications entre les détenteurs des dossiers permet de partager les fichiers constitués par un organisme à une fin bien précise avec d'autres utilisateurs qui poursuivent des fins bien différentes. On donne à ce processus le nom de raccordement des données.

L'impact possible, sur la protection de la vie privée, de la facilité avec laquelle les dossiers sont extraits, partagés et fusionnés se trouve multiplié par le nombre et la diversité des sources de renseignements informatisés sur les individus. Matériellement, les ordinateurs sont passés en vingt ans de l'état de machine de la taille d'une pièce à celui d'appareil facile à poser sur un bureau. Les coûts de l'équipement et du traitement ont baissé à la même allure. Pour se servir des anciens ordinateurs, il fallait avoir une formation poussée; les machines actuelles, qualifiées d'aimables pour l'utilisateur, peuvent être utilisées avec un minimum de formation et de connaissances spécialisées.

Alors qu'autrefois, seules les institutions importantes, comme les gouvernements, disposaient des ressources nécessaires pour utiliser l'ordinateur de façon efficace, la tenue de dossiers informatisés est maintenant la norme dans presque tous les secteurs de l'activité humaine. Autrefois, le recensement national était l'unique compilation de renseignements divers sur les citoyens. Il est maintenant possible de rassembler des données encore plus diverses sur les individus, en partageant les informations entre les détenteurs de dossiers. Au gouvernement, le dossier de chaque personne comprend, entre autres, des renseignements sur l'état-civil, l'impôt, le casier judiciaire, la santé, la conduite automobile, les dossiers militaires et les dossiers scolaires.

Dans le secteur privé, les renseignements sur les individus qui figurent dans les dossiers informatisés sont encore plus variés. Parmi les plus connus, citons le dossier de solvabilité. Le public se préoccupe cependant de la constitution d'autres dossiers informatisés, notamment dans les secteurs des assurances, de la banque et des télécommunications. Il y a en outre beaucoup d'utilisateurs de données encore inconnus du public comme les détaillants qui ont un système de cartes de crédits ou les services d'achat par télévision, les magazines qui gardent les listes d'abonnement, les organismes de bienfaisance, commerciaux,

professionnels ou communautaires et autres prestataires de services. Maintenant que la télédistribution entre dans une phase d'échange où il va être possible de se servir de la télévision pour procéder à ses opérations bancaires, faire ses achats, effectuer des sondages instantanés et commander les émissions de télévision sur la base du coût unitaire, le secteur privé va accumuler des quantités encore plus importantes de renseignements sur les individus.

Cette collection toujours grandissante de données personnelles est un élément quasi inévitable de la vie en ce dernier quart du vingtième siècle. Comme concluait, en 1977, une commission d'étude sur la protection de la vie privée aux États-Unis :

Il est maintenant courant de demander à un particulier de donner des renseignements sur lui-même qui seront utilisés par des étrangers invisibles, lesquels prendront des décisions à son sujet qui influenceront sur sa vie quotidienne. De plus, comme la majorité des services offerts par les organismes sont, ou du moins sont considérés comme des nécessités, le particulier n'a guère le choix et doit se soumettre à toutes les exigences des organismes qui lui posent des questions.

Pratiques loyales en matière d'information

Cette menace pour la protection de la vie privée a suscité un certain nombre de tentatives visant à fixer les limites appropriées et à protéger le caractère confidentiel des renseignements personnels conservés dans les systèmes informatisés. Les principes généraux énoncés dans la convention du Conseil de l'Europe sur la protection des individus en matière de traitement automatique des données personnelles sont un bon exemple des efforts tentés par les gouvernements pour établir des lignes directrices qui reconnaissent les avantages de la tenue de dossiers informatisés tout en respectant la valeur que les particuliers accordent à leur vie privée.

Ces lignes directrices sont basées sur les principes suivants :

- i) Les renseignements personnels doivent être recueillis et traités de façon loyale et légitime.
- ii) Les renseignements personnels doivent être conservés à une fin ou à des fins spécifiées et légitimes.
- iii) Les renseignements personnels ne doivent pas être utilisés ni divulgués d'une manière incompatible avec lesdites fins.
- iv) Les renseignements personnels doivent être adéquats, pertinents et d'une portée qui ne dépasse pas les fins spécifiées.
- v) Les renseignements personnels doivent être exacts et, le cas échéant, remis à jour.
- vi) Les renseignements personnels ne doivent pas être conservés sous une forme où figure le nom de la personne plus longtemps que nécessaire pour les fins spécifiées.
- vii) Le sujet concerné par les renseignements doit avoir accès aux données qui existent sur son compte et être habilité à les corriger ou à les radier si les dispositions légales régissant lesdites données n'ont pas été respectées.
- viii) Des mesures de sécurité appropriées doivent être prises contre l'accès sans autorisation, l'altération ou la dissémination, la perte accidentelle ou non autorisée des données.

Ces directives reconnaissent qu'il est nécessaire, pour l'individu, que les renseignements recueillis à son sujet le soient avec son consentement; que ce consentement soit basé sur une pleine et précise compréhension des fins auxquelles les renseignements sont recueillis; qu'il n'en soit pas fait usage sans son consentement; qu'il puisse avoir accès au fichier pour s'assurer que les renseignements sont corrects;

qu'en cas de désaccord sur l'exactitude des renseignements, sa version des faits soit notée et que des tiers n'aient pas accès à son dossier sans qu'il le sache ou le permette, sauf si c'est exigé par la loi.

Même s'il y a accord général sur ces principes dans les deux secteurs public et privé, il existe un certain nombre d'obstacles à leur réalisation. L'un de ces obstacles est le principe voisin de la liberté de l'information. Si un individu a le contrôle absolu sur toutes ses données personnelles, ce droit peut constituer un obstacle important au droit qu'ont les autres de se renseigner sur les activités gouvernementales. Il faut de toute évidence trouver un moyen terme.

Le problème du vol des données informatiques constitue un autre obstacle. Il s'agit du cas où des données sont saisies ou extraites sans la permission du détenteur du fichier de renseignements. On a suggéré d'apporter des amendements au Code criminel qui établiraient des infractions spécifiques en la matière et permettraient de résoudre en partie le problème. Les détenteurs de banques de données devraient cependant continuer à prendre des précautions raisonnables, au sein de leur organisation, pour faire en sorte que soit respecté le caractère confidentiel des renseignements personnels, et que les employés qui les manipulent se conforment aux mesures de sécurité nécessaires.

Le problème du passage des données d'un territoire à l'autre constitue un troisième obstacle en puissance. Il s'agit des renseignements sur des particuliers qui sont extraits et traités dans un autre territoire où la protection de la vie privée n'est pas assurée comme il se doit par le secteur privé ou par la loi. Ici aussi, l'efficacité et la valeur de la liberté de l'information risquent d'entrer en conflit avec les normes sur la protection des données personnelles. Certains de ces problèmes dépassent la portée de la présente discussion, car ils relèvent du gouvernement fédéral.

Perceptions du public

Des sondages récents indiquent que l'inquiétude devant la menace que représente, pour la protection des renseignements personnels, l'utilisation grandissante des ordinateurs n'est pas l'unique apanage des professeurs, des futurologues et des technocrates. Des sondages effectués pour le compte du gouvernement de l'Ontario en 1980 et 1983¹ indiquent qu'une majorité considérable de citoyens de l'Ontario sont préoccupés par l'impact des ordinateurs sur leur vie privée. En outre, en 1983, environ la moitié d'entre eux estimaient qu'il incombe essentiellement au gouvernement de protéger le caractère confidentiel des renseignements personnels et financiers dans notre société. Trente-huit pour cent des citoyens pensaient que c'était au secteur privé de protéger leur vie privée. Le premier sondage, effectué en 1980, révélait en outre qu'une minorité considérable de citoyens estimaient que les institutions comme le gouvernement, les dispensateurs de crédit, les employeurs et les compagnies d'assurance demandent aux particuliers trop de renseignements personnels et financiers.

Dans le même ordre d'idée, un sondage Gallup² de 1981 sur les attitudes envers la microélectronique demandait à la population de classer par ordre d'importance treize problèmes associés aux ordinateurs et à la technologie de l'information. La protection de la vie privée et le respect du caractère confidentiel des renseignements personnels venaient loin en tête et étaient mentionnés par 63% des personnes interrogées. Le nombre de gens ayant un pouvoir de contrôle sur l'information, problème étroitement lié au premier, était mentionné par 45 pour cent des personnes interrogées, ce qui classait cette préoccupation en troisième position. C'étaient les personnes qui déclaraient

-
1. Voir Ontario Consumer Issues 1980 et Préoccupations du consommateur ontarien en 1983
 2. A Gallup Survey of Electronic Technology, mars 1981, The Gallup Organisation, Inc.

avoir des connaissances en microélectronique et les titulaires d'emplois dans le secteur de la vente, du travail de bureau et de l'administration qui se montraient le plus préoccupées par la protection de la vie privée. On demandait également aux personnes interrogées de se projeter cinq ans en avant et de dire si elles pensaient que leur vie privée serait alors "envahie ou gravement perturbée" par l'une ou plusieurs de dix-sept organisations, personnes morales ou individus. Le niveau d'inquiétude était élevé. Cinquante pour cent ou plus des personnes morales suivantes risquaient, à leur avis, d'envahir leur vie privée : une agence d'évaluation de la solvabilité, un ordinateur ou une banque de données, une compagnie d'assurance, le gouvernement fédéral ou provincial, une banque, une personne qui pourrait s'ingérer dans leur courrier et une autre qui communiquerait avec elles par téléphone. Une fois de plus, ce sont les personnes qui déclaraient connaître la microélectronique qui étaient le plus susceptibles de prévoir une invasion de leur vie privée.

Un sondage effectué en novembre 1982 à London, Ontario, par le professeur Neil Vilmar de l'université Western Ontario³, pour le compte du gouvernement de l'Ontario, a révélé des niveaux pareillement élevés d'inquiétude pour la vie privée devant le développement des services interactifs de télédistribution. Plus des deux-tiers des personnes interrogées pensaient que leur vie privée était moins protégée au Canada que dix ans plus tôt. Parmi les types d'informations considérées les plus délicates et nécessitant le plus de protection, on citait les comptes en banque, le contrôle des entrées et des sorties de chez soi (câblotransmission utilisée par certains systèmes de sécurité), les dossiers de crédit, le salaire personnel et les dossiers médicaux. Les résultats indiquaient que près de la moitié des personnes interrogées s'inquiétaient de l'usage que faisait le gouvernement des renseignements recueillis, mais un pourcentage encore plus élevé était préoccupé par le secteur privé. Soixante-douze pour cent de l'échantillon

3. Neil Vedmar, Privacy and Two-way Cable Television: A Study of Canadian Public Opinion, Université Western Ontario, 1983.

donnaient la faveur à une réglementation par le gouvernement, une majorité de cinquante-deux pour cent accordant un rôle en la matière aux deux gouvernements fédéral et provincial. L'étude révélait également que la plupart des gens estimaient que les organismes publics et privés demandent davantage de renseignements personnels que nécessaire.

Réponse du secteur privé

Comme l'indiquent les directives de l'Organisation pour la coopération et le développement économique,⁴ l'auto-réglementation des industries et des compagnies qui font un usage important de renseignements personnels constitue un des principaux moyens de protéger efficacement la vie privée des citoyens. À cet égard, plusieurs compagnies ont relevé le défi de l'auto-réglementation en établissant des pratiques internes bien pensées correspondant à la définition courante des pratiques loyales en matière d'information établie, entre autres, par l'OCDE.

Bell Canada, par exemple, est une corporation importante qui manipule une quantité considérable d'informations personnelles nécessairement recueillies aux fins de facturation. Les politiques de la compagnie considèrent tous les renseignements de l'abonné à l'exception de son nom, de son adresse et de son numéro de téléphone, comme des informations privées conservées uniquement pour répondre aux besoins au sein de la compagnie. Les données personnelles ne peuvent pas être vendues et les employés de Bell sont informés que tout renseignement sur les abonnés, où qu'ils soient recueillis, sont strictement confidentiels. En fait, l'existence, le contenu ou la nature de toute communication de l'abonné ne doit pas être communiqué à un tiers sauf pour se conformer à une ordonnance légale. Dans le cas d'une telle ordonnance, Bell avisera l'abonné, à moins qu'on ne le lui défende spécifiquement.

4. Organisation pour la coopération et le développement économique, Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data.

La Banque de Montréal est un autre utilisateur de données personnelles qui a mis au point des pratiques spécifiques de protection des renseignements personnels et publié des informations à ce sujet. Les données recueillies et gardées en dossier constituent le minimum nécessaire pour dispenser le service requis. Au sein de la compagnie, l'accès à ce type de renseignement est étroitement contrôlé et aucune information n'est généralement fournie à un tiers sans le consentement du client, sauf pour se conformer à la loi ou à une ordonnance du tribunal. Les demandes de carte de crédit, les prêts personnels et les hypothèques, cependant, comprennent une clause de consentement général ou de renonciation qui autorise la banque à divulguer des renseignements sur le client à des tiers dans certaines circonstances. La pratique qui consiste à faire signer des renonciations aux clients, courante dans les institutions financières, a été critiquée dans le passé au nom de la protection de la vie privée du client.

Le secteur de la télédistribution du Canada a chargé son association, l'Association canadienne de télédistribution, de mettre au point un code général de protection des renseignements personnels qui lui permettra de s'auto-réglementer. Un sous-comité de l'association, sur le modèle du code hautement respecté de l'institution américaine de câblodiffusion Warner Amex, est en train d'élaborer un code correspondant à la scène canadienne. On prévoit que ce code sera accepté et appliqué par les compagnies membres de l'association alors qu'elles mettent au point les services interactifs qu'elles vont offrir au public. L'établissement d'un code avant le développement des services présente un avantage majeur, car les systèmes peuvent être conçus à l'avance pour renforcer la sécurité informatique et les possibilités de protection des données.

Il n'en demeure pas moins que les compagnies pourvues d'un code de protection volontaire constituent l'exception plutôt que la règle. Il est donc clair que la vaste manipulation informatisée des renseignements personnels devra être assujettie à un système de normes quelconque pour veiller à ce que la vie privée des citoyens ne soit pas violée.

PARTIE II : LOIS RÉGISSANT LES BANQUES DE DONNÉES
DU SECTEUR PUBLIC

Le nombre de lois visant, au Canada et à l'étranger, à répondre aux problèmes que posent l'accès à l'information et la protection des renseignements personnels va croissant. La plupart sont d'origine récente, ce qui est révélateur de leur rapport étroit avec le développement de la technologie de l'information et de la rapidité avec laquelle les innovations risquent de soulever de graves questions en matière de protection de la vie privée. Dans cette section seront passées en revue un certain nombre de solutions, dont certaines ne s'attachent qu'aux banques de données gouvernementales alors que d'autres visent également le secteur privé.

Canada

Au niveau canadien national, l'effort porte essentiellement sur l'élaboration de pratiques loyales en matière d'information dans les fichiers relevant de la compétence fédérale. La Loi sur la protection des renseignements personnels, adoptée en 1982 et proclamée en 1983, confère aux citoyens canadiens et aux résidents permanents le droit d'être informés, à certaines exceptions près, de l'existence de dossiers à leur sujet, d'examiner, de corriger et de remettre en question les renseignements qui s'y trouvent; de savoir quel usage a été fait du dossier; et d'être consultés avant qu'il en soit fait un autre usage. Une loi voisine, la Loi sur l'accès à l'information a été édictée pour maximaliser la compatibilité entre l'accès à l'information et la protection de la vie privée. La Loi sur la protection des renseignements personnels exige que soit publié un répertoire annuel des fichiers fédéraux de données personnelles et crée un Commissaire à la protection de la vie privée habilité à jouer le rôle du médiateur en cas de litige, à enquêter pour veiller à ce que la loi soit observée par les détenteurs de fichiers et à exercer son droit de recours en révision devant la Cour des décisions gouvernementales touchant lesdits renseignements.

Provinces

La Nouvelle-Écosse et le Nouveau-Brunswick ont édicté l'une et l'autre des lois sur la liberté de l'information vers la fin des années 1970. La loi de Nouvelle-Écosse énumère les types de documents auxquels on peut avoir accès plutôt que d'établir un principe général d'accès, alors que le Nouveau-Brunswick établit des principes généraux, avec possibilité d'appel à un ombudsman et inspection à huit-clos des documents contestés par les tribunaux.

La Nouvelle-Écosse a adopté des lois sur la liberté de l'information et la protection des renseignements personnels en 1981. La première loi dresse la liste des ministères, conseils, organismes et commissions visés et l'autre fait de la violation, par une personne, de la vie privée d'un individu un tort exécutoire sans preuve de dommage.

Le Québec traite en même temps la liberté d'information et la protection des renseignements personnels dans une loi adoptée en 1982 et destinée, comme la loi fédérale, à protéger les données personnelles contenues dans les fichiers gouvernementaux, tout en permettant l'accès aux documents des organes publics. Ces organes comprennent non seulement le gouvernement provincial et tous ses ministères et organismes, mais aussi les municipalités (gouvernement et institutions gouvernementales aux paliers du comté, de la région et de la ville), les établissements d'enseignement et les institutions de santé et de services sociaux. La loi exige que la commission d'accès à l'information compile aux fins de circulation un répertoire des dossiers tenus par les organes publics et que les demandes d'information reçoivent gratuitement une réponse dans les 20 jours qui suivent leur réception. La commission a des pouvoirs divers de supervision, d'enquête et de décision.

Dans le passé, l'Ontario a sérieusement étudié les questions d'accès à l'information et de protection des renseignements personnels. Il en est résulté un projet de loi, le Privacy and Access to Information Bill, visant à définir les pratiques loyales en matière d'information et à les rendre obligatoires dans les fichiers de renseignements personnels du gouvernement. Le projet prévoit d'établir un bureau de la protection des données qui aurait le pouvoir d'élaborer et de faire appliquer des normes auxquelles seraient assujettis les systèmes de données personnelles. Ces normes exigeraient, entre autres, que soit limitée la collecte de données au minimum essentiel à l'opération d'un programme; que les renseignements personnels soient normalement recueillis directement auprès du sujet et que la raison de la collecte lui en soit communiquée; et, de manière générale, que les renseignements recueillis ne soient pas divulgués sans le consentement de l'individu. Feraient exception à la règle relative à la divulgation les cas où celle-ci ne représenterait pas une ingérence injustifiée dans la vie privée de l'individu et où elle serait nécessaire à l'administration de programmes gouvernementaux autorisés ou au meilleur intérêt de l'individu ou de la société. Les particuliers auraient le droit d'accéder à leur dossier et d'y apporter des corrections, le détenteur des données étant tenu de notifier les utilisateurs passés du dossier de tout amendement à celui-ci. Les particuliers auraient également le droit de porter plainte devant le bureau séparé d'un commissaire.

En 1968, la Colombie-Britannique a adopté une loi sur la protection des renseignements personnels, ce qui en a fait le premier gouvernement du Commonwealth à établir un recours indépendant en cas d'ingérence déraisonnable et injustifiée dans la vie privée d'un individu. Cette loi a été suivie par des textes semblables au Manitoba et en Saskatchewan. Cependant, aucune de ces lois ne traite expressément de l'utilisation inappropriée ou non autorisée des renseignements personnels donnés volontairement à une autre personne ou à une autre institution et intégrés dans un fichier informatisé.

De plus, le coût du recours aux tribunaux risque de faire hésiter l'individu à se prévaloir de ses droits, les coûts du procès dépassant souvent ses avantages possibles.

États-Unis

La loi américaine sur la protection des renseignements personnels date de 1974 et vise les données personnelles contenues dans les fichiers gouvernementaux. Il s'agit essentiellement d'un texte à fonctions domestiques qui établit des normes pour l'administration des fichiers de données. À cet égard, il exige du gouvernement qu'il fasse rapport sur l'existence de fichiers de renseignements personnels, qu'il veille à la qualité des données qui s'y trouvent, qu'il permette aux sujets de ces fichiers d'y avoir accès, d'utiliser uniquement les données aux fins pour lesquelles elles ont été recueillies et de tenir un dossier de la divulgation des informations aux personnes concernées. Les réponses aux questions ne sont pas limitées dans le temps et la loi s'applique d'elle-même dans la mesure où la personne lésée saisit les tribunaux de sa plainte plutôt que de s'adresser à une instance séparée. Les États-Unis ont également une loi sur la liberté de l'information qui confère des droits d'accès relativement plus étendus que la loi sur la protection des renseignements personnels.

Royaume-Uni

Le parlement britannique est en train d'élaborer une loi sur la protection des données qui vise les fichiers informatisés de renseignements personnels des deux secteurs public et privé. Ce projet établit un registraire et un tribunal de protection des données; exige l'enregistrement (à certaines exceptions près) des fichiers de renseignements personnels publics et privés; prohibe la divulgation non autorisée des informations; permet aux particuliers d'avoir accès aux données détenues dans les fichiers enregistrés et les habilite à amender les dossiers et à chercher compensation auprès des tribunaux en cas de préjudice.

Le registraire est habilité à annuler l'enregistrement des fichiers de renseignements personnels qui contreviennent aux principes de protection desdites données et peut empêcher le transfert de renseignements du Royaume-Uni dans un pays qui ne respecte pas les normes minimales en la matière. Cette loi permettra au Royaume-Uni d'adhérer à la convention du Conseil de l'Europe sur la protection des données.

République fédérale de l'Allemagne occidentale

La République fédérale allemande n'a pas de loi générale sur l'accès à l'information mais un réseau hautement développé de dispositions visant à protéger les renseignements personnels et à sauvegarder la vie privée des individus. Il s'agit d'une part de la loi fédérale sur la protection des renseignements personnels et des lois des états sur le même sujet qui intègrent les principes de protection des données du Conseil de l'Europe. La loi fédérale vise également les fichiers de renseignements personnels du secteur public fédéral et du secteur privé à l'échelle du pays, alors que les lois des états régissent les pratiques en la matière de leurs gouvernements respectifs. C'est aux directeurs des institutions gouvernementales qui créent et utilisent les fichiers de renseignements personnels qu'il incombe en priorité de veiller au respect des lois. De même, les lois du palier fédéral et des états prévoient la mise en place du bureau d'un commissaire à la protection des données personnelles, chargé de superviser et de conseiller les organismes qui manipulent des fichiers de renseignements personnels et de faire rapport au parlement une fois par an. Le succès de ce système de protection ne vient pas des pouvoirs de coercition de la commission à la protection des renseignements personnels mais du degré élevé de sensibilisation du public et du gouvernement aux pratiques appropriées en matière de manipulation des données.

Suède

La Suède a été le premier pays du monde à promulguer des lois sur l'accès à l'information et la protection des renseignements personnels. L'accès aux renseignements détenus par le gouvernement est réglementé par la loi sur la liberté de la presse et la loi sur la protection des renseignements personnels qui, ensemble, permettent l'accès général dans le cadre de certaines exceptions spécifiques et limitées. Le caractère confidentiel de l'information est garanti par plusieurs textes législatifs dont le plus important est la loi sur les données personnelles de 1973. Cette loi a créé une commission d'inspection des renseignements personnels qui réglemente la collecte et l'utilisation des fichiers informatisés dans les deux secteurs public et privé. La fonction majeure de la commission est donc de délivrer des permis à tous les fichiers de renseignements détenus par le gouvernement ou par les utilisateurs du secteur privé et d'édicter des règlements qui régissent leur usage. On peut appeler des décisions de la commission au ministre de la justice et au cabinet, mais le nombre de ces appels n'a jamais été élevé. De façon générale, le système qui régit l'utilisation des renseignements fait passer la protection de la vie privée avant les considérations d'économie et d'efficacité.

Conseil de l'Europe

Le Conseil de l'Europe a préparé une convention pour la protection des individus relativement au traitement automatisé des renseignements personnels, qui vise à assurer le respect du droit de l'individu à la protection de sa vie privée. Elle requiert des états signataires qu'ils intègrent dans leurs lois nationales les principes de base définis dans la convention à savoir : emploi de pratiques loyales en matière d'information; limites imposées à l'utilisation et au contenu des fichiers en fonction des fins auxquelles les données sont recueillies; exactitude; identification minimale des individus; limites imposées aux types de données à traiter; mesures de sécurité appropriées;

et procédures pour permettre aux sujets des dossiers d'identifier ces derniers, de les examiner et de les corriger. La convention confirme également le droit qu'ont les états signataires de refuser que des renseignements personnels soient envoyés dans des pays n'offrant pas une protection similaire.

Organisation pour la coopération et le développement économique. (OCDE)

Le Conseil de l'OCDE a établi des directives régissant la protection des renseignements personnels qui constituent les normes minimales que doivent respecter ses membres. Sur le modèle de la convention du Conseil de l'Europe, l'OCDE souscrit aux principes suivants: limite de la collecte, qualité des données, spécification des fins auxquelles elles sont utilisées, limitation de l'utilisation, mesures de sécurité, ouverture, participation individuelle, responsabilité. Tout en énonçant spécifiquement que la protection des renseignements personnels ne doit pas servir d'alibi pour limiter leur passage au-delà des frontières, l'OCDE convient que les pays membres doivent empêcher toute exportation de données qui circonviennent les lois nationales sur la protection des renseignements personnels ou dans des pays ne respectant pas en substance les principes auxquels il souscrit. Les pays membres sont invités en particulier à : adopter des lois nationales appropriées; encourager et soutenir l'auto-réglementation; conférer aux individus un moyen raisonnable d'exercer leurs droits; prévoir des sanctions adéquates; et veiller à ce que les sujets des dossiers ne fassent pas l'objet de discriminations injustes.

Résumé

On a pu voir dans ce qui précède que les diverses lois édictées par différentes autorités couvrent un très vaste territoire. La plupart souscrivent à un ensemble similaire de pratiques et de principes loyaux en matière d'information.

Bien qu'il y ait divergence sur des points de détail, lorsqu'il s'agit par exemple de décider si les renseignements recueillis doivent être "pertinents" et recueillis "directement", la plupart des lois confèrent à l'individu le droit d'accès et de correction et exercent un certain contrôle sur la transmission des renseignements personnels à un tiers. Au-delà de ces similarités de base, cependant, ces lois varient énormément au niveau de leur portée et de leur application.

Aux fins de ce document, il paraît utile de prendre acte de trois des modèles discutés ci-dessus. À une extrémité du spectre, la loi américaine sur la protection des renseignements personnels est un exemple de loi qui définit certains droits individuels mais n'établit pas d'organe séparé pour en assurer le respect. Aux termes de cette loi, c'est à l'individu de saisir les tribunaux de ses griefs.

Un second modèle, illustré par la Loi canadienne sur la protection des renseignements personnels, établit un organe d'exécution nanti de pouvoirs d'enquête et de contrôle. Les particuliers lésés peuvent porter plainte auprès du Commissaire à la protection de la vie privée qui peut également prendre l'initiative d'une plainte et exercer le recours en révision pour refus de communication. La nouvelle loi du Québec est assez semblable, bien que son champ d'application soit plus vaste et couvre notamment les municipalités, les conseils scolaires, les universités et les organismes de santé et de service social, en plus des ministères du gouvernement. La loi du Québec confère à sa commission le pouvoir considérable de surveiller les pratiques en matière d'information, d'instruire les plaintes, de faire enquête et de rendre des ordonnances de force exécutoire.

Le troisième modèle, à l'autre extrémité du spectre, est illustré par le système d'enregistrement du Royaume-Uni décrit ci-dessus. Sous certains aspects, ce système de réglementation est plus fort que les deux modèles

précédents, car il requiert l'enregistrement formel des fichiers de renseignements personnels et confère au registraire des pouvoirs substantiels d'enquête et d'application, notamment le pouvoir de refuser d'enregistrer un fichier si son utilisateur ne se conforme pas aux dispositions de la loi. Les systèmes d'enregistrement suédois et allemand vont encore plus loin et constituent deux modèles supplémentaires.

PARTIE III : SOLUTIONS POSSIBLES POUR LE SECTEUR PRIVÉ

Résumé des problèmes

La première partie de ce document exposait la menace que constitue pour la vie privée des citoyens la manipulation automatisée des renseignements personnels. Il s'en dégage un certain nombre de notions concurrentes. La plupart des gens conviennent qu'il faut pondérer les avantages de l'ordinateur en matière d'efficacité et de vitesse par l'évaluation de ce qu'il en coûte au niveau de la protection de la vie privée des individus. En termes d'économie, les institutions commerciales sont donc soumises à des pressions conflictuelles qui visent d'une part à profiter de toutes les économies que permet de réaliser la technologie nouvelle et, d'autre part, à garantir à l'individu la protection des renseignements personnels le concernant.

Bien qu'il soit difficile de généraliser, il appert que le coût de la protection minimale de la vie privée n'est pas très élevé par rapport aux économies que la nouvelle technologie permet de réaliser au niveau de l'efficacité. De plus, ces coûts de "protection" sont souvent minimisés si l'on fixe des normes ou des procédures avant d'introduire les nouveaux systèmes.

Les problèmes exposés dans la partie I peuvent se résumer comme suit :

- 1) Collecte des données : Les renseignements personnels recueillis par les utilisateurs de données⁵ doivent-ils se limiter à ce qui relève spécifiquement

5. Les définitions suivantes sont utilisées dans ce document : Utilisateur de données : Institution qui recueille et manipule des fichiers de renseignements personnels sur les particuliers. Sujet des données : Individu qui fait l'objet de la collecte de données.

de l'objectif de l'utilisateur et à ce qui a fait l'objet du consentement éclairé du sujet? Faudrait-il exiger en outre que les renseignements personnels soient recueillis directement auprès du sujet auquel ils se rapportent? Les principales déclarations de principe sur le problème de l'obtention des données sont généralement assorties d'une clause à l'effet que ces dernières doivent être recueillies en toute justice et légitimité, à une fin elle-même légitime. Ce document part du principe que la légitimité ne constitue pas un problème et s'attache à la pertinence de la collecte des données et au consentement éclairé du sujet.

- 2) Qualité des données : Les renseignements personnels recueillis par les utilisateurs de données doivent-ils être assujettis à des exigences d'exactitude, de complétude et de remise à jour?
- 3) Limitations de la divulgation : La communication, par les utilisateurs de données, de renseignements personnels à des tiers doit-elle se limiter aux renseignements requis pour atteindre l'objectif spécifié par l'utilisateur? Feraient exception à cette règle les cas où il y a consentement du sujet ou ceux qui tombent sous le coup de la loi.
- 4) Mesures de sécurité : Les utilisateurs de données doivent-ils obligatoirement veiller à la sécurité physique des fichiers de renseignements personnels?
- 5) Accès individuel : Les particuliers doivent-ils avoir le droit de vérifier l'existence de dossiers personnels à leur sujet, d'inspecter et de recevoir une copie des renseignements qui y sont contenus et de demander que soient modifiées les données erronées ou incomplètes?

- 6) Coûts : Si l'on donne aux citoyens le droit d'accès, de modification et de non-divulgaration, les coûts d'application de ces droits ne doivent pas être rédhibitoires. Les règlements qui confèrent à des organismes d'application de la loi le pouvoir quasi judiciaire de régler les griefs constituent un moyen de conférer aux particuliers des droits susceptibles d'être respectés.

Cette section analyse un certain nombre de solutions aux problèmes qui se posent dans le secteur privé et passe en revue les points forts et les faiblesses de chacune. On part du principe que la protection des renseignements personnels est une exigence légitime et que les principes énoncés par la convention du Conseil de l'Europe sur la protection des données (résumés en page 5) représentent une référence raisonnable pour l'évaluation des solutions proposées.

Portée du document

Ce document vise les deux secteurs, public et privé. Du point de vue du citoyen individuel, les deux secteurs représentent une menace pour la protection de la vie privée. Bien qu'en Amérique du Nord, les lois sur la protection des renseignements personnels n'aient visé jusqu'à présent que le secteur public, des pays comme le Royaume-Uni⁶, l'Allemagne de l'Ouest et la Suède ont des programmes législatifs qui couvrent les deux secteurs.

La question du choix se présente alors entre l'auto-réglementation et la réglementation gouvernementale. On examinera ci-dessous les avantages et les inconvénients de l'auto-réglementation comme moyen de garantir que le secteur privé adopte des pratiques loyales en matière d'information.

6. Au moment de la rédaction de ce rapport, le projet de loi britannique avait été accepté en seconde lecture

Il est une autre question que les gouvernements doivent régler. Il faut en effet décider si les programmes de réglementation doivent couvrir seulement les fichiers informatisés de renseignements personnels ou s'appliquer à tous les dossiers, aussi bien manuels qu'informatisés. Le principe majeur du livre blanc⁷ du Royaume-Uni sur la protection des données est que l'automatisation présente de nouvelles menaces pour la protection de la vie privée, à cause de la vitesse et de la facilité avec laquelle les renseignements personnels peuvent maintenant être communiqués à un coût relativement peu élevé. Cela sous-entend que l'argent et les efforts que demande le transfert manuel des renseignements freinent d'eux-mêmes la divulgation non autorisée.

En revanche, les lois sur la protection des données qui visent les dossiers du secteur public d'Amérique du Nord ne distinguent pas entre fichiers informatisés et dossiers manuels. Ces lois confèrent à l'individu certains droits en matière de protection des renseignements personnels dans les deux types de dossier. On peut se rendre compte de l'importance des dossiers manuels dans le cas, par exemple, des archives médicales.

Il faut également se demander si tous les fichiers de renseignements personnels devraient être couverts par la réglementation imposée ou l'auto-réglementation, ou seulement ceux dont la taille dépasse un certain seuil. Certains insistent sur le fait que seuls les utilisateurs de données d'une certaine importance devraient être assujettis à la réglementation, les coûts d'application constituant un fardeau plus élevé pour les organismes moins importants. L'exemption des banques de données plus petites, cependant, laisserait ces renseignements sans protection et affaiblirait par là même les droits individuels.

7. Data Protection: The Government's Proposals for Legislation, ministère de l'Intérieur, Royaume-Uni, avril 1982.

Politiques possibles

Cette section passe en revue quatre solutions possibles : un code volontaire de protection des renseignements personnels, un code aux termes d'une loi, un système d'enregistrement et de réglementation, et une méthode combinant les éléments des trois premières propositions. Cette liste n'a pas la prétention d'être exhaustive mais vise à encourager la discussion des diverses solutions qui semblent raisonnablement correspondre à la situation canadienne.

1) Code volontaire de protection des renseignements personnels : Une fois admise la légitimité de la protection des données personnelles, les gouvernements pourraient inciter les industries spécifiques (par le biais de leurs associations) et les corporations qui font un usage important de données à élaborer des codes volontaires qui intégreraient les principes importants qui figurent habituellement dans les lois sur la protection de la vie privée. Des compagnies comme Warner-Amex aux États-Unis et IBM en Europe ont déjà mis au point des directives pour la protection des renseignements personnels contenus dans leurs fichiers. Au Canada, l'Association canadienne de télédistribution est en train d'élaborer un code.

En 1981, Warner-Amex Cable Communications Inc. a mis au point un code visant à protéger le caractère confidentiel des renseignements personnels que la compagnie compile sur les abonnés au service de télédistribution. Dans ce code, la compagnie s'engage à garantir la sécurité matérielle et le caractère confidentiel des renseignements sur les abonnés et à informer ces derniers de toutes les fonctions des services de télédistribution qui donnent lieu à une collecte de renseignements. Un accord passé avec chaque abonné énonce les conditions d'utilisation des renseignements et prévoit que nulle autre donnée individuelle ne sera recueillie sans le consentement de l'individu. Le code donne également à l'abonné le droit d'examiner son dossier et d'exiger la correction des données erronées.

Le code est en train de s'intégrer aux contrats et aux accords de franchise passés avec les abonnés, ce qui le rend auto-applicable et confère à l'abonné certains droits. En théorie, tout individu qui estime que son droit à la protection de sa vie privée a été violé peut intenter des poursuites pour bris de contrat.

Commentaires : On peut résumer de la manière suivante les avantages et les inconvénients de la méthode du code volontaire en réponse aux problèmes posés par la protection des renseignements personnels;

- Elle ne garantit pas que la majorité des institutions qui font un usage important de données adopteront volontairement un code.
- Elle ne propose pas de système formel d'application ni de respect des codes (à l'exception du pouvoir limité qu'a le particulier d'intenter des poursuites pour bris de contrat, dans le cas où le code est assorti d'un accord écrit entre l'utilisateur et le sujet des données).
- Les coûts et difficultés qu'elle entraîne pour les utilisateurs de données sont minimaux.
- Elle présente une flexibilité maximale, les codes pouvant s'adapter à l'évolution de la technologie et des exigences du public.
- Elle ne garantit pas de droits substantiels à l'individu en cas de litige sur l'accès, la correction ou la divulgation.
- L'adoption de divers codes volontaires par divers secteurs et compagnies industriels risque d'aboutir à un manque d'uniformité de la protection offerte aux individus.

2) Code imposé par la loi : À mi-chemin entre les codes volontaires et les règlements gouvernementaux plus traditionnels, une autre méthode propose d'édicter une loi qui définirait les pratiques loyales en matière d'information et prévoirait des pénalités pour toute

infraction à ces pratiques. Lesdites pratiques pourraient couvrir la collecte et la qualité des données, les limites à la divulgation, les mesures de sécurité et l'accès individuel tels que définis ci-dessus. Cette loi permettrait d'intenter une action délictuelle au civil et constituerait essentiellement une méthode d'auto-réglementation du problème sans le secours d'un organe d'exécution.

Certains auteurs ont suggéré que les exigences du public en matière de protection de la vie privée viennent de ce que les parlements et tribunaux n'ont pas déjà élaboré ce type de loi⁸. On convient généralement que la common law en vigueur dans les pays du Commonwealth n'offre pas en soi de protection de la vie privée.

Les lois sur la protection des renseignements personnels édictées par la Colombie-Britannique, la Saskatchewan et le Manitoba n'ont pas souvent été utilisées et, de l'avis général, ne proposent pas de remède substantiel au type de problème que pose à l'individu la manipulation automatisée des données personnelles.

Une loi prévoyant un code de protection des renseignements personnels pourrait prendre l'une des deux formes suivantes :

- a) Une loi qui permettrait l'acceptation volontaire du code. Les règlements afférents à ce type de loi enregistreraient les industries ou compagnies qui souhaitent se conformer au code. Les participants volontaires seraient ainsi identifiés dans leur secteur comme des compagnies conscientes des problèmes de protection de la vie privée.
- b) On peut aussi songer à une loi qui exigerait le respect du code. Elle s'appliquerait à tous les utilisateurs de données ou seulement aux fichiers de renseignements personnels dont l'importance dépasse un certain seuil.

8. Voir par exemple, Roger Noll, "Regulation and Computer Services", dans M. Dertouzos et J. Moses, The Computer Age: A Twenty-Year Review, (Cambridge: MIT Press, 1980) et Murray Rankin, Privacy and Technology: A Canadian Perspective (Canadian Institute for Legal Studies, Cambridge University, 1983).

Commentaires: On trouvera ci-dessous un résumé des points forts et des faiblesses de cette méthode:

- . Elle ne garantit pas qu'une majorité des utilisateurs de données se conformera volontairement au code. Seule la version obligatoire d'un tel statut garantit la participation d'une majorité des utilisateurs de données.
- . Le remède proposé aux particuliers est coûteux et compliqué. Il ne serait sans doute pas souvent utilisé, les coûts pour le particulier dépassant presque toujours les avantages possibles du remède. Il s'ensuit que cette approche ne confère pas de droits substantiels à l'individu relativement à l'accès, la correction, la divulgation des renseignements et la résolution des litiges.
- . Les coûts et les complications pour les utilisateurs de données sont minimaux.
- . La méthode offre un degré élevé de flexibilité, les pratiques loyales en matière d'information étant définies dans la loi en termes généraux qui ne gêneraient pas l'application de nouvelles techniques.
- . Si le recours des particuliers au remède prévu reste limité, ce type de loi n'aura pas d'impact majeur sur les pratiques en matière d'information. La version obligatoire de ce type de loi, cependant, peut favoriser une certaine uniformité dans la collecte générale des données et les pratiques générales en matière de divulgation.

3) Enregistrement et réglementation : Une autre solution possible au problème serait que les gouvernements édictent des lois qui exigent l'enregistrement des fichiers de renseignements personnels, donnent aux individus des droits d'accès et de correction bien définis; réglementent la collecte de renseignements personnels et leur divulgation à des tiers; garantissent la sécurité des données; et établissent un registraire habilité à faire enquête et à faire appliquer la loi. L'exigence d'enregistrement pourrait s'appliquer aux institutions qui constituent des fichiers informatisés de renseignements personnels.

C'est là, fondamentalement, la méthode adoptée par le Royaume-Uni dans le projet de loi sur la protection des données (Data Protection Bill) présenté dans la deuxième partie de ce document. Ce texte institue un système d'enregistrement et d'application de la loi à l'intention des usagers de fichiers informatisés de renseignements personnels. Bien que le système d'enregistrement s'applique également au secteur public et au secteur privé, sa structure fondamentale peut servir de modèle utile aux fins de discussion.

Dans ce modèle, le répertoire public des utilisateurs de données sensibilise les individus à l'existence des fichiers informatisés de renseignements personnels et aux objectifs qu'ils visent. L'utilisateur de données doit s'identifier, dire quels renseignements il utilise, d'où ils proviennent, à qui ils sont communiqués et à quelles fins ils sont utilisés. Le registraire a le pouvoir de faire enquête, d'inspecter les dossiers et d'exiger des modifications au système. Dans les cas extrêmes, il peut refuser l'enregistrement pour non-conformité aux termes des grands principes de protection des renseignements personnels prévus par la loi. Étant donné les pouvoirs étendus du registraire, ce type de loi institue un processus d'appel à un tribunal indépendant composé d'experts en droit et en informatique.

Le texte proposé par le Royaume-Uni donne également à l'individu le droit d'accès aux renseignements personnels; le droit à la compensation pour préjudice causé par l'utilisation de données erronées, la perte de données et la divulgation non autorisée ainsi que le droit de recours aux tribunaux pour demander la rectification ou la radiation des données incorrectes. C'est au particulier de saisir les tribunaux de sa plainte en cas de violation de ses droits individuels pour exiger le respect de la loi ou réclamer des dommages-intérêts.

D'autres dispositions du même texte permettent au gouvernement de restreindre le transfert de certaines catégories de renseignements dans des pays spécifiés où la protection des données ne fait pas l'objet d'une réglementation aussi stricte, d'autoriser l'établissement de règlements pour régir certaines catégories de données personnelles comme l'origine raciale, les appartenances politiques et les croyances religieuses; et d'exempter des dispositions de la loi les collectes de données effectuées aux fins de recherches, si les individus ne sont pas identifiables.

Les commentaires suivants ne s'attachent qu'aux caractéristiques générales d'un système d'enregistrement de ce type tel qu'il serait appliqué au secteur privé. Il ne s'agit pas d'une évaluation de l'ensemble du texte.

Commentaires : Les avantages et inconvénients de cette méthode peuvent se résumer comme suit :

- . Elle prévoit aux termes de la loi la protection des renseignements personnels recueillis par les utilisateurs les plus importants et l'assortit d'un mécanisme chargé de faire observer ladite loi.
- . Elle confère à l'individu des droits légaux d'accès et de correction ainsi que de protection contre la divulgation à des tiers. En cas de litige, cependant, la défense de ces droits peut s'avérer coûteuse pour l'individu qui doit s'adresser aux tribunaux.
- . Elle impose de nouveaux règlements au secteur privé, c'est-à-dire des coûts supplémentaires aux utilisateurs.
- . Elle permet une certaine souplesse car les principes de protection des données sont généraux tout comme les pouvoirs du registraire, ce qui leur permet de s'adapter à l'évolution de la technologie et des pratiques en matière d'information.
- . Le système d'enregistrement et les pouvoirs d'exécution auraient un effet marqué sur les pratiques en matière d'information.

Les systèmes d'enregistrement sont courants dans les lois sur la protection des renseignements personnels des autres pays européens. On a donné, dans la deuxième partie, une brève description des lois de l'Allemagne de l'Ouest et de la Suède, sans doute les deux exemples les plus dignes d'intérêt.

L'inconvénient majeur de ce modèle, du point de vue de l'individu, est ce qu'il lui en coûte de s'adresser au tribunal pour faire respecter ses droits. Un autre système d'enregistrement pourrait comporter, pour le citoyen, une possibilité d'appel à un registraire ou à un commissaire dont les ordonnances auraient force exécutoire pour l'utilisateur de données. Ceci résoudrait le problème du coût rédhibitoire pour le particulier.

De nombreuses provinces canadiennes ont édicté des lois qui réglementent la collecte et la divulgation des renseignements personnels en matière de crédit. En Ontario, par exemple, la loi sur les renseignements concernant le consommateur enregistre les bureaux de crédit, réglemente la collecte, la conservation et la divulgation des renseignements en matière de crédit et confère à l'individu le droit d'accès à son dossier de crédit personnel. Le registraire est habilité à révoquer ou à refuser l'enregistrement dans certaines circonstances, auquel cas le candidat peut faire appel à un tribunal. Les modèles utilisés par les provinces pour réglementer les renseignements en matière de crédit pourraient fournir une orientation au système d'enregistrement envisagé pour les utilisateurs de fichiers de renseignements personnels.

4. Enregistrement volontaire : On pourrait envisager d'autres possibilités en combinant les trois approches ci-dessus. Une méthode digne d'intérêt consisterait à combiner les deux systèmes d'auto-réglementation et d'enregistrement. Les associations industrielles pourraient élaborer des codes de protection des renseignements personnels qui correspondent à leur secteur, veiller à ce que

leurs membres honorent lesdits codes et servir de médiateur en cas de plaintes de la part des citoyens. Ceci pourrait se faire en consultation avec un bureau public de la protection de la vie privée qui tiendrait également un registre de toutes les associations et compagnies membres.

Commentaires : On trouvera ci-dessous un résumé des points forts et des faiblesses de ce type de méthode :

- . Comme dans le modèle d'auto-réglementation, cette méthode ne garantit pas que la majorité des utilisateurs de données adopteront volontairement le système d'enregistrement.
- . Elle établit un système de surveillance visant à encourager les compagnies et organismes participants à observer le code. Bien que cette approche puisse avoir beaucoup de poids, elle ne prévoit pas d'autorité formelle en matière d'observation ni d'exécution.
- . Elle entraîne des coûts supplémentaires pour les utilisateurs de données.
- . Elle offre un niveau de flexibilité élevé et permet à l'industrie et à l'organisme de coordination de s'adapter à l'évolution de la technologie et des pratiques en matière d'information.
- . Elle ne garantit pas de droits concrets à l'individu en cas de litige sur l'accès, la correction ou la divulgation. L'organe d'instruction des plaintes des associations professionnelles pourrait cependant jouer un rôle de médiation.
- . Bien que l'adoption de différents codes par différents secteurs crée certaines variations au niveau des normes sur la protection de la vie privée, l'organisme de coordination pourrait viser l'uniformité sur les questions importantes comme le droit de l'individu à l'accès, à la correction et à la non-divulgation.

Résumé

On s'est efforcé dans cette section de comparer l'efficacité de plusieurs méthodes qui pourraient être utilisées pour résoudre les problèmes de la protection des renseignements personnels dans le secteur privé. Plutôt que de passer en revue toutes les approches possibles, y compris les systèmes gouvernementaux les plus stricts d'enregistrement et de délivrance de permis, ce document s'est attaché aux méthodes qui semblent convenir davantage à la scène canadienne.

On trouvera à la page suivante un tableau comparatif des quatre méthodes décrites ci-dessus. Les critères utilisés pour les comparaisons sont basés sur l'analyse précédente en fonction du thème majeur de toute discussion sur les choix en matière de réglementation : l'équilibre entre les coûts pour l'industrie et l'établissement de droits individuels ou de mesures de protection pour les citoyens. Les termes "bas", "moyen" et "élevé" cherchent uniquement à donner une idée des valeurs relatives de chaque système.

ÉVALUATION DES SOLUTIONS POSSIBLES

SOLUTIONS

CRITÈRES DE BASE	CODE DE PROTECTION VOLONTAIRE	CODE IMPOSÉ PAR LA LOI	ENREGISTREMENT ET RÉGLEMENTATION	ENREGISTREMENT VOLONTAIRE
Coûts pour l'utilisateur de données	Bas	Bas	Moyens à élevés	Moyens
Flexibilité	Élevée	Moyenne	Moyenne	Élevée
Droit du particulier à l'accès, à la correction et à la non-divulgaration	Sans garantie	Droits garantis par version obligatoire de la loi	Droits légaux pour les particuliers	Pas de garantie
Droits du particulier en cas de litige	Aucun	Coûteux et difficile à appliquer pour le particulier	Coûteux à appliquer D'autres systèmes d'enregistrement pourraient pallier ce problème	Aucun
Uniformité des pratiques en matière d'information	Difficile à assurer	Possible dans version obligatoire	Encourage uniformité	Certaine uniformité possible
Efficacité pour le développement de normes générales de protection	Basse à moyenne	Basse à moyenne	Potentiel élevé	Moyenne

BA1
I4
- C52

DOCUMENT: 870-123/005

INTERPROVINCIAL CONFERENCE ON PRIVACY:
INITIATIVES FOR 1984 (SYMPOSIUM)



ABSTRACT

Fair Information Practice and Computers

Hugh V. O'Neill
President,
American Society of Access Professionals

Toronto, Ontario
May 23-24, 1984

ABSTRACT

Fair Information Practice

and

Computers

Hugh V. O'Neill
President, American Society of
Access Professionals

BACKGROUND OF FAIR INFORMATION PRACTICE

U.S.
More than a decade ago, an advisory committee to the⁴ Department of Health, Education and Welfare issued a fundamental statement of information policy and practice in a report called "Records Computers and the Rights of Citizens."

The July 1973 report of the Advisory Committee on Automated Personal Data Systems found that, at that time, a person's privacy was poorly protected against arbitrary or abusive record-keeping practices. To safeguard the privacy of individuals and in recognition of the need to establish standards of record-keeping practices appropriate to the computer age, the report recommended the enactment, by Congress, of a Federal Code of Fair Information Practice" for all automated personal data systems.

The five basic principles on which the Code rests are as follows:

1. There must be no personal data record-keeping systems whose very existence is secret.
2. There must be a way for an individual to find out what information about him/her is in a record and how it is used.
3. There must be a way for an individual to prevent information about him/her that was obtained for one purpose from being used or made available for other purposes without his/her consent.
4. There must be a way for an individual to correct or amend a record of identifiable information about him/her.
5. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data.

There are certain exceptions to these principles in the interest of some greater need--a couple of examples:

1. There are times when individuals should not be given access to records on themselves, e.g., in order to protect confidential sources in investigations or in the interest of national security.
2. There are times when other societal goals outweigh the need for privacy, and that in such cases information should be disclosed and used without the consent of the individual for purposes other than the specific purpose for which the information was originally collected, e.g., in compelling circumstances affecting the health or safety of a human being, including life-threatening situations.

A balance must be struck so that all statutes, regulations, and policies controlling personal information incorporate the basic principles of the canon while at the same time permit society's other goals to be effectively and efficiently achieved.

- o The connection of government and private sector computerized data banks
- o International computer networks cross the boundaries of national law.

CONCLUSION

Considerable effort has been expended to attempt to maintain adequate and reasonable safeguards for the use of computerized information systems. The legislative and executive branches have both tried to implement the fair information practice principles. However, there is a need for a continuing and even an increased level of effort, if we are to use the most advanced computer-communications technology and still protect the rights of individuals.

RECOMMENDATIONS

The following initiatives for 1984 and beyond:

- o Enacting Federal legislation and designing model state statutes for computer protection/crime situations
- o The use of computer technology for the implementation of fair information practice principles, example: access to an index of personal data files through remote user terminals, computer techniques to enhance security
- o The design of safeguards for computer applications especially for computer-matching and screening--general safeguards in legislation, more detailed safeguards in regulations and policy statements
- o Follow-up, audit, evaluation to ensure that practice follows the legislative, regulatory and policy safeguards
- o The drafting of second generation fair information practice statutes (The Privacy Act of 1974 is an example of a first generation fair information practice statute)
- o The establishment of an entity with adequate resources and priority to:
 - assist in the above recommendations
 - to perform long-range planning--trying to lock the barn door before the horse is stolen
 - assist in the controlled sharing of computerized information.

In sum, both the entity in the executive branch and the legislative branch should work toward the implementation of a proper balance so that statutes, regulations, and policies controlling personal information incorporate the basic principles of fair information practice while at the same time permit society's other goals to be effectively and efficiently achieved.

DOCUMENT: 870-123/005

Traduction du Secrétariat

CONFÉRENCE INTERPROVINCIALE SUR LA PROTECTION
DES RENSEIGNEMENTS PERSONNELS:
MESURES POUR 1984 (COLLOQUE)

RÉSUMÉ

Les pratiques loyales en matière d'information
et le secteur de l'informatique

Hugh V. O'Neill
Président
American Society of Access Professionals



Toronto (Ontario)
Les 23 et 24 mai 1984

RÉSUMÉ

Les pratiques loyales en matière d'information
et le secteur de l'informatique

Hugh V. O'Neill
Président,
American Society
of Access
Professionals

HISTORIQUE DES PRATIQUES LOYALES EN MATIÈRE D'INFORMATION

Il y a plus d'une décennie, un comité consultatif auprès du U.S. Department of Health, Education and Welfare rendait public un énoncé fondamental de la politique et des pratiques en matière d'information dans un rapport intitulé "Records Computers and the Rights of Citizens".

D'après le rapport publié en juillet 1973 par le Advisory Committee on Automated Personal Data Systems, à cette époque la vie privée d'une personne était bien mal protégée contre les pratiques arbitraires ou abusives relatives à la tenue de dossiers. Afin de respecter la vie privée des personnes et de reconnaître la nécessité d'établir des normes de pratiques en matière de tenue de dossiers qui soient adaptées à l'ère de l'informatique, le rapport recommandait que le Congrès adopte un code fédéral des pratiques loyales en matière d'information pour tous les systèmes informatisés renfermant des données personnelles.

Le code en question repose sur cinq principes fondamentaux:

1. Il ne doit y avoir aucun système de données personnelles dont l'existence même est tenue secrète.
2. Une personne doit avoir le moyen de savoir quels sont les renseignements qu'un dossier renferme sur son compte et comment ils sont utilisés.
3. Une personne doit avoir le moyen d'empêcher que des renseignements qui avaient été obtenus à son sujet pour une raison bien précise soient utilisés ou communiqués pour d'autres fins sans son consentement.
4. Une personne doit avoir le moyen de corriger ou de modifier les données identifiables qu'un dossier renferme à son sujet.
5. Toute organisation qui constitue, maintient, utilise ou diffuse des dossiers renfermant des données personnelles identifiables doit s'assurer de la véracité des données pour l'usage auquel elles sont réservées et doit prendre les précautions requises pour en empêcher la mauvaise utilisation.

Il existe certaines exceptions à ces principes dans l'intérêt d'un besoin supérieur, par exemple:

1. Il y a des cas où les personnes ne devraient pas avoir accès aux dossiers qui les concernent, par exemple pour protéger des sources confidentielles en cours d'enquête ou dans l'intérêt de la sécurité nationale.

2. Il y a des cas où d'autres buts touchant la société sont plus importants que la nécessité de protéger la vie privée, et en pareil cas, il y a lieu de divulguer et d'utiliser ces renseignements sans le consentement de la personne à des fins autres que le but précis pour lequel les renseignements avaient été recueillis au départ, par exemple, dans des circonstances exceptionnelles touchant la santé ou la sécurité d'un être humain, notamment lorsqu'il s'agit d'une question de vie ou de mort.

Il importe d'établir un équilibre de sorte que tous les règlements, lois et politiques contrôlant les données personnelles intègrent les principes fondamentaux du code tout en permettant la réalisation efficace et réelle des autres objectifs de la société.

Les deux ensembles d'objectifs peuvent être atteints par le respect du principe de l'application régulière de la loi, y compris le caractère ouvert du processus de prise de décisions. Les exceptions aux principes du code ne devraient être autorisées que lorsque la population en a été avertie, soit lors d'audiences du Congrès ou des assemblées législatives des États, soit par des avis des règlements prévus, des réunions publiques et dans des documents spécialisés et la presse en général. Il est essentiel que les parties intéressées, y compris la population lorsque cela convient, aient la possibilité de participer pleinement au processus de prise de décisions, par exemple en ce qui a trait à la décision d'utiliser ou de divulguer des renseignements à des fins autres que celles pour lesquelles les données avaient d'abord été recueillies.

Les décisions autorisant des exceptions aux droits à la vie privée garantis aux personnes par les principes du code ne devraient être prises qu'au palier de gouvernement le plus élevé et le plus responsable et prendre la forme d'une loi fédérale ou d'État, d'une ordonnance exécutive présidentielle, d'une ordonnance du gouverneur, ou d'une règle ou d'un règlement officiel, de façon que le public soit pleinement informé des mesures prises.

La Privacy Act de 1974 constituait la première étape législative de la mise en oeuvre de ces principes au niveau fédéral. Pour ce qui est des États, dix d'entre eux ont jusqu'ici adopté une loi exhaustive sur la protection de la vie privée, intitulée soit "Privacy Act" ou "Fair Information Practice Act". Il s'agit des États suivants: l'Arkansas, la Californie, le Connecticut, l'Indiana, le Massachusetts, le Minnesota, l'État de New York, l'Ohio, l'Utah et la Virginie.

LA TECHNOLOGIE DE L'INFORMATIQUE - 1984 ET LES ANNÉES À VENIR

Il convient de relever les caractéristiques suivantes:

- o Accroissement de la vitesse d'exécution - on s'oriente vers le milliard d'opérations à la seconde et vers une mémoire à plus forte capacité.
- o La cinquième génération d'ordinateurs comprendra l'intelligence artificielle.
- o Réseaux informatisés - ordinateur central avec terminaux
- o Réseau d'ordinateurs - interconnexion d'importants systèmes centraux de traitement de données
- o Réseau de banques de données axées sur un seul domaine d'intérêt
- o Réseau de banques de données axées sur toute une gamme d'intérêts
- o Ordinateurs personnels, ordinateurs au foyer, machines de traitement de textes fonctionnant tant à l'intérieur de réseaux que de façon autonome
- o Problèmes tant techniques qu'administratifs suscités par la sécurité des ordinateurs - crime à la hausse dans le domaine de l'informatique
- o Recours au jumelage d'ordinateurs afin de comparer les dossiers que renferment différentes banques de données au sujet de millions de personnes - fonctionnement à divers paliers de gouvernement: fédéral, État et local
- o Raccordement des banques de données informatisées des secteurs public et privé
- o Les réseaux informatisés internationaux dépassent les limites des lois nationales.

CONCLUSION

Des efforts considérables ont été consacrés aux mesures visant à maintenir des garanties raisonnables et appropriées pour l'utilisation des systèmes de renseignements informatisés. Les corps législatif et exécutif ont tous deux tenté d'appliquer les principes de pratiques loyales en matière d'information. Cependant, il importe de poursuivre ces efforts, voire de les

augmenter, si nous voulons utiliser les techniques de communication faisant appel aux ordinateurs les plus perfectionnés tout en protégeant les droits des particuliers.

RECOMMANDATIONS

Mesures à prendre en 1984 et au-delà:

- o Adoption de lois fédérales et élaboration au palier des États de lois modèles pour la protection des données informatisées et la lutte contre le crime dans ce secteur
- o Le recours aux techniques d'informatique pour la mise en oeuvre des principes de pratiques loyales en matière d'information, par exemple: accès à un répertoire des dossiers de données personnelles grâce à des terminaux pour usagers éloignés, techniques d'informatique visant à accroître la sécurité
- o Établissement de garanties dans le domaine de l'informatique, en particulier pour le jumelage et le sondage d'ordinateurs - garanties générales dans la loi, garanties plus détaillées dans les règlements et dans les énoncés de principe
- o Suivi, vérification, évaluation afin que la pratique respecte les garanties législatives, réglementaires et de principe.
- o Rédaction d'une deuxième génération de lois relatives aux pratiques loyales en matière d'information (la Privacy Act de 1974 constitue un exemple d'une loi de "première génération".)
- o Création d'une instance dotée de ressources et de priorités appropriées et chargée:
 - de favoriser la mise en oeuvre des recommandations susmentionnées;
 - d'effectuer une planification à long terme - mieux vaut prévenir que guérir;
 - de contribuer à la mise en commun contrôlée des données informatisées.

En résumé, l'instance responsable du secteur exécutif et le secteur législatif devraient travailler de concert à l'établissement d'un juste équilibre de sorte que les lois, règlements et politiques relatifs aux données personnelles intègrent les principes fondamentaux de pratiques loyales en matière d'information tout en permettant la réalisation efficace et efficiente des autres objectifs de la société.

DOCUMENT: 870-123/006

CA1
24
-C52

INTERPROVINCIAL CONFERENCE ON PRIVACY:
INITIATIVES FOR 1984 (SYMPOSIUM)

Why Computer Scientists
and the Computing Profession
Must Work to Shape Impending Legislation

(From: Proceedings, Canadian Information Processing Society
Sessions '84)

Rodney H. Cooper,
Department of Computer Science, University of New Brunswick
and Wayne Patterson,
Département de Mathématique, Physique et Informatique,
Université de Moncton



Toronto, Ontario
May 23-24, 1984

WHY COMPUTER SCIENTISTS AND THE COMPUTING PROFESSION

MUST WORK TO SHAPE IMPENDING LEGISLATION

Rodney H. Cooper* and Wayne Patterson**

*Dept. of Computer Science, University of New Brunswick, Fredericton, NB

**Dept. de Mathématique, Physique, et Informatique, Université de Moncton, Moncton, NB

ABSTRACT --- This paper is divided into three sections: In the first, the authors review pending legislation affecting the computing profession in Canada, the United States, and Great Britain. In the second section, areas of potential future legislation in Canada are explored. In the final section are some illustrations of the dangers involved in the passage of legislation that has not had the careful scrutiny of computer science and the computing profession.

RESUME --- L'article est divisé en trois sections: Dans la première section, les auteurs examinent les projets de loi actuels au Canada, aux Etats-Unis, et en Grande-Bretagne qui touchent l'informatique. Dans la deuxième section, on étudie la possibilité des possibles futurs projets de loi au Canada. Dans la dernière section, on donne quelques exemples des dangers qui peuvent se produire si des lois que les informaticiens n'ont pas bien scrutées sont adoptées.

"Images of Fear, Images of Hope" --- those words correctly describe what computing professionals should see when they regard the emerging public policy interest in the conduct of our profession.

The profession should consider it very hopeful that various governments in Canada and elsewhere are now beginning to address issues of signal importance to our profession and to society as a whole. This legislative activity clearly indicates that the impact of our profession is now generally understood, and that it is time to open the question of computer-related legislation.

The purpose of this paper is threefold: First, a review will be given of existing legislative initiatives in Canada, in the provinces, and also in the United States and Great Britain.

second section will deal with potential areas of legislative interest.

The third and final section will indicate several images of fear for the computing community. It will be our contention that computer scientists must become much more active participants in the development of

related public policy; for, as we shall see, legislation developed in the absence of appropriate technical considerations may result in unfortunate conclusions even when the legislative principles are laudable. We will indicate this concern by citing several examples and by indicating some precautions that could be followed.

A. Present Legislation

This part will be divided into five subdivisions: Canada, the provinces, the United States, the individual States of the United States, and Great Britain.

1. Canada

At present, the only pending legislation before the House of Commons is Bill C-19 [1], which would create two new offences in the Criminal Code of Canada. The first is for the unauthorized use of a computer: "Everyone who dishonestly ... (a) obtains, directly or indirectly, any computer service, (b) by means of an electromagnetic, acoustic, mechanical or other device, intercepts or causes to be intercepted, directly or indirectly, any function of a computer system, or (c) uses or causes to be used, directly or indirectly, a computer system with intent to commit an offence is guilty of an indictable offence and is liable to imprisonment for a term not exceeding ten years, or is guilty of an offence punishable under summary conviction" [1].

The second offence is for "mischief in relation to data": "Every one commits mischief who wilfully (a) destroys or alters data; (b) renders data meaningless, useless or ineffective; (c) obstructs, interrupts or interferes with the lawful use of data; or (d) obstructs, interrupts, or interferes with any person in the lawful use of data or denies access to data to any person who is entitled to access thereto." [1] Mischief in relation to data is also punishable by ten years or summary conviction. At the time of this writing, the Bill (introduced on February 7, 1984) had not proceeded to the committee stage, that is, the major discussion of the Bill had not yet taken place.

However, the purpose of the pertinent sections of C-19 have been praised by the computing community

Until now, it has been very difficult, if not impossible, for the owner of a computer system to seek legal remedy should the system be penetrated by unauthorized users using electronic means. The most celebrated case before Canadian courts is *Regina v. McLaughlin* [2], where an original conviction of theft of information was overturned on appeal.

Hopefully, the current provisions, subject to a caveat in the third section of this paper, will provide greater grounds for prosecution.

In addition to Bill C-19, private member's bills on computer security had been introduced in the 32nd Parliament [3], [4].

There are also working groups in several federal departments studying possible areas of legislation. These include: trans-border data flow, copyright law, and a Canadian response to the Fifth Generation Computer initiatives. Furthermore, the Justice and Legal Affairs Standing Committee of the House of Commons last year held hearings and published a report on computer crime and other matters.

Pertinent documents on these latter areas are referenced in [3], [6], and [7].

2. Canadian Provinces

The authors wrote to all Canadian Attorneys-General recently to inquire as to relevant pending provincial legislation. At the time of this writing, the only provinces with responses indicating the existence of computer-related legislation were Nova Scotia and Manitoba. The Manitoba Attorney-General indicated that Freedom of Information legislation was in the process of being developed. [8]

To quote from our response from Nova Scotia: "We do have a general provision in our Freedom of Information Act, c. 10, S.N.S., 1977, respecting the privacy of information contained in a department [of the Provincial Government] file. In addition, under our Consumer Reporting Act, c.4, S.N.S., 1973 the Legislature has enacted restrictions on the information and its use that may be stored on a file in respect of a consumer and the disclosure of such information. 'File' is defined so that it applies regardless of the manner or form in which the information is stored." [9]

3. United States

In large measure because of the nature of the Congressional system, there is a proliferation of computer-related legislation. In fact, at least 46 bills are now before the Congress on computer-related issues. The major categories of legislation are: computer literacy, computer crime,

small business computer security, research on computer security and privacy, robot research and manufacturing, protection of the copying of silicon masks, and tariff on disc drive spindles.

A complete summary of this legislation given in Appendix A. Conversations with legislators and aides in Washington indicated a fair likelihood of passage of "computer literacy" bill. There are competing approaches to this legislation.

One approach (the Stark Bill or "Apple Bill") provides for tax deductions for computer manufacturers who contribute computers to schools and other not-for-profit institutions. The other approach (the Wirth Bill) provides appropriations for school computer programs -- for the purchase of hardware, software and provisions for teacher training.

The other broad area of legislation which has had a great deal of discussion is an area of computer security. Extensive hearings were held [10] on September 1983, and October 17 and 24, 1983, on this issue; but, at present, because of opposition from the Department of Justice and the FBI, the various bills addressing this issue are unlikely to go forward.

It is interesting to contrast the response of the computing profession in Canada to the United States to computer crime legislation. In Canada, the profession seems to be solidly behind a computer crime bill, whereas in the United States there seems to be either benign interest or quiet opposition [11].

Other, non-legislative issues explored by the Congress include the de-monopolization of telecommunications facilities (break-up of the telephone companies) and manufacture of supercomputers.

4. The States

At the time of this report, twenty states had passed some form of computer crime bill including Arizona, California, Colorado, Delaware, Florida, Georgia, Illinois, Massachusetts, Michigan, Minnesota, Montana, New Mexico, North Carolina, Ohio, Rhode Island, South Dakota, Tennessee, Utah, Virginia, and Wisconsin. [12]

In addition, California has passed a version of the so-called "Apple Bill": computers (one per school) have been consequently donated by the Apple Corporation.

5. Great Britain

There is only one relevant piece of legislation before the British Parliament.

--- the so-called Data Protection Bill [13]. This bill has (twice) in 1983 passed the House of Lords, and is currently before the House of Commons.

The purpose of the Data Protection Bill in the British Parliament is to provide a protection for the privacy of the individual with respect to information on that individual contained in various private- and public- sector data banks.

Fundamentally, this bill will require the management of data banks to have these banks licensed. The licensing process will presumably contain requirements for the security of the computer system and also for respecting privacy rights of the individual and permitting access to the individual.

The view of the government is that this legislation is required owing to the explosion of information contained in computers; the opposition has argued that the legislation has only been proposed because of a requirement of the European Economic Community for data protection legislation; that, absent this requirement, British industry might find itself at a disadvantage in doing business in Europe.

Major points of contention in the debate on this bill have been: 1) the fact that only computerized files, not manual files, fall under the scope of the Bill; 2) that one individual, rather than an agency, has the responsibility of enforcement of the legislation; 3) that certain types of government information are exempt from the bill's provisions; and 4) the methods of making known to the public what information about them is held in various computer banks.

B. Potential Areas of Legislation

The impact of computer- and micro-electronics-based technology on society is enormous. Clearly it will become much greater.

In any society, as the impact of a set of practices affects more and more members of the society, conflicts inevitably grow, and, in a democratic society, institutions of the common weal, such as governments, must decide on methods of anticipating and regulating these conflicts.

Governments seem, by their nature, to act slowly and deliberately. Thus many changes in society brought about by new technologies have not yet been addressed by government. It is the purpose of this article to indicate some of these areas of existing and potential conflict.

Privacy

We have deliberately placed this issue at the head of our list. A number of surveys [14] have indicated that the principal concern of the Canadian public, with regard to new technologies, is the fear of invasion of privacy (rather than loss of employment, which is usually described by the news media as the principal fear).

In Canada, there is virtually no legislation which specifically protects the citizen from invasions of privacy now possible by virtue of increasingly larger amounts of data being stored in computer systems.

With respect to the government's own treatment of information, there are laws and regulations which prohibit, for example, the use of information in one government department by another. (The UIC cannot, for example, regularly search Revenue Canada records to find out if beneficiaries have secret employment.)

However, it is doubtful that many Canadians would find solace in principles established before the advent of computers.

For example, suppose the UIC and Revenue Canada decided to use the same data base management system to combine accounts, save space, machine resources, and tax dollars. Should this be permitted? Would it represent an inherent violation of privacy? What if the DBMS were of a sufficiently advanced technology that reading another department's records was, say, more costly in resources than breaking into that other department's offices (or computers)?

In any case, it seems there are no current standards for computer privacy and security inside the federal government or any provincial government. What is needed, as a first step, is the establishment of such standards, both to prevent government abuse, and also abuse by outside intervention.

As a minimum, legislation should be developed to require the encryption of all data deemed to be of a confidential nature, and, as a bare minimum, that all data concerning individual citizens be considered to be of that confidential nature. [16]

As a consequence, it would seem necessary to establish procedures to develop a Canadian data encryption standard.

Citizens are concerned not only about government collection of information, but also of information gathered by the private sector.

Similar standards as described above should also be adopted by, or legislated for, the banking, credit, insurance, and health industries. It is always more feasible for an industrial sector to regulate itself, yet

legislation should require that the industrial standards should meet if not exceed the standards that government imposes upon itself.

Computer Crime

Theft using the computer has grown to be big business. From the pettiest example of the college student copying someone else's program, to the "hacker" destroying valuable files, to the professional thief altering accounts, computer crime has been pervasive, difficult to detect, and often unpunishable. The landmark Canadian *Regina v. McLaughlin* case [2] showed the difficulty of prosecution.

As described above, the Minister of Justice for Canada, the Honourable Mark MacGuigan, has recently introduced legislation[1] which will permit any unwarranted intervention into a computer system to be considered a crime, punishable by up to ten years' imprisonment.

One problem with this legislation will be enforcement. As with most of Canada's Criminal Code, establishment of the offence lies in the federal jurisdiction, while the responsibility for enforcement resides with the province.

At present, there is little expertise in provincial law enforcement agencies in the detection and prosecution of computer-related offenses.

Copyright

Copyright law is a venerable concept in the British legal system. In recent years it has been under fire as technology has strained it to its limits.

The preoccupation with copyright increased a few years ago when photocopiers came into widespread use. When, if ever, is it legal to copy a book?

This question gained additional significance with the introduction about fifteen years ago of popularly-priced audio recording devices; and recently the concern has been intensified with the introduction of video recorders.

The same fundamental phenomenon has also occurred with respect to digital media. For all of the above technologies, it is important, and legitimate, to have low-cost copying mechanisms.

When the copying mechanisms exist, and when there are economic advantages to copying, it will be done.

There are two questions to be considered in further legislation on copyright:

Are there different tests or standards to be applied in determining what copying computer software is legitimate? (Probably so: Only with disks is accidental erasure of stored information likely.)

Second, are there quantitative standards determining plagiarism (as opposed to mere copying)? This question is undoubtedly infinitely more complex when dealing with software.

Presumably, specialists in art or literature detection or literary theft can determine when an author, painter, or composer has plagiarized from another.

But trying to do the same with a program using a public algorithm, may be impossible or difficult.

It should be noted that the Canadian Department of Justice has a task of studying this issue currently.

International Data Flow

Another area of potential legislative activity is in what is called trans-national data flow.

Canada should be legitimately concerned to whether or not unregulated flow of information across national borders is in the national or the public interest.

The Department of Communications has studied this question.

There are currently many industries that depend on the storage and/or treatment of data in foreign computers.

The first question to be decided is, therefore, a strategic national interest: ensuring that "Canadian" data is in some way under Canadian control. For example, would there to be a Canadian security standard could or should it be imposed on data stored in foreign computers?

The second question to be asked is economic in nature. Should data collected in Canada be permitted to reside on foreign computers? If so, it is not hard to visualize a time when "data havens" emerge, much as certain countries have become known as "tax havens."

This second issue is also clearly related to the question of free trade versus protectionism.

A final but related issue concerns government interest in data that may be collected and stored in foreign computers but yet used by Canadians. Current examples would include the online data banks such as Dialog, BRS, and CompuServe.

An important study on this issue has been done for the Royal Bank of Canada [3], [6].

Professional Certification and Accreditation

As the computing profession matures, the question of professional certification will become a subject of legislative interest.

If the pattern followed by other professions is repeated, this certification will fall under provincial jurisdiction. Bar Associations, Medical Societies, Associations of Professional Engineers, are all regulated and given authority by provincial legislatures, although the various societies themselves often are grouped into national associations.

Legislation certifying professionals in other professions includes a process of accreditation of degree-granting programs

CIPS has initiated a program of accrediting university degree programs in computer science [17]. Canada thus is further advanced than the United States, where the ACM is studying accreditation but has not yet embarked on any accreditation projects.

The computing profession as a whole must decide whether or not it is in its best interest to seek professional status through legislation

An alternative is that governments may decide that such certification and regulation is necessary and thus impose it on the profession.

Computers in the Schools

Another area of activity within provincial governments in Canada, and with more than a passing interest at the federal level is the subject of computers in the school curriculum.

Provincial ministries of education are rushing to provide computers in schools. In general, this development has proceeded without legislation

The views on the use of computers in schools in our profession are extremely diverse, ranging from Seymour Papert's "computers are pencils" concept [18] to the views of many computer scientists that computer science should not be taught at all at the pre-college level

There are many aspects of the use of computers in schools that could become the subject of legislation. Provinces could, for example, mandate the teaching of computer science or "computer literacy".

Provinces may also set standards for the qualifications of teachers teaching of computer-related courses; which, at present, do not exist.

Computer Ethics

Last year, the Standing Committee on Justice and Legal Affairs of the House of Commons [7] reported on a number of issues involving the use of computers

Among their recommendations was one suggesting that courses on computer ethics be taught --- at the school level and the university level

This issue clearly overlaps with the two preceding items, but is included here because of the specific reference from the Standing Committee.

Wiretapping

There is currently extensive legislation concerning wiretapping in Canada

What must be studied is whether or not existing legislation in this regard is sufficiently broad to cover the wiretapping of data communications lines.

It should be noted that the above are only a few of the issues which may well come under legislative scrutiny in the forthcoming months and years. It should be mentioned in conclusion that other issues to consider are: The definition of a letter and how this affects Canada Post and electronic mail; legislation concerning job displacement and retraining, the entry of Canada into fifth-generation technology [20]; and legislation concerning the use of robots in industry.

C. The Responsibility of The Computing Profession

Careful examination of virtually all of the legislation described in section A above demonstrates why it is critically important that the computer science and the computing profession must monitor and intervene in the development of all legislation that will affect our community

Computer-related legislation requires a thorough knowledge of technical questions that is not often possessed by non-professionals.

As a consequence, there is a grave danger that legislation developed by non-computer-scientists may inadvertently create loopholes or otherwise lead to unexpected results. We will cite five examples drawn from the legislation mentioned in section A to illustrate this point

1. The Definition of a Computer Program

In Bill C-19 of the House of Commons of Canada [1], as discussed above, provisions for establishing "computer crime" are set out. In the definition of terms of this legislation is the following: A "'computer program' means data representing instructions or statements that, when executed in a computer system, causes the computer system to perform a function"

This definition must be very carefully scrutinized. A naive view of programming languages is that they consist of a series of "statements" or "instructions" that executed in sequence cause a certain task to be carried out. Indeed, this model of programming languages is consistent with the von Neumann model of a computer.

However, it is equally true that many computer languages do not have statements or instructions. Languages that are based on the von Neumann model are often called "imperative languages" [21]. Another class of languages, however, are the "functional" or "applicative" languages. In such a language, a program is not a series of statements but rather, a function. Execution of the program is done by applying the function to its arguments. Examples of applicative languages include LISP, Prolog, and (according to some authors), APL.

The danger of using the above definition to define "computer programs" should be evident. It is not difficult to conceive of the destruction of a LISP program --- or perhaps an entire artificial intelligence project --- not falling under the criminal code because of a defence establishing that LISP programs were not "computer programs" according to the C-19 definition.

A remedy in this case is not difficult, however, since the examination of the Bill indicates that it could be rewritten without necessarily mentioning computer programs (that is, distinguishing programs from other types of data). This temporary solution would not be applicable when it becomes necessary to define computer programs in copyright legislation.

2. One Computer, One Student?

One of the important bills before the United States Congress is HR 3750 (Wirth, D-Colorado), "The Computer Literacy Act of 1983", which has its purpose "to promote computer literacy among elementary and secondary school students and their teachers" [22]. This bill would provide appropriations for school districts to purchase computers, software, and provide for teacher training.

In addition, the bill requires that the funds be allocated according to the greatest need, that is, that "funds be provided first to those schools with the least computer

hardware per student . . . funds are provided to any school after such school the equivalent of one unit of computer hardware for each thirty children"

"Computer hardware" is then further defined in such a way as to indicate that computer equals one unit of computer hardware. The bill's authors have not taken into account the possibility of a multi-user system being an attractive option on a school purchase, this is undoubtedly because almost all discussion of school computing has been in the context of single-user microcomputers such as Apple II's, TRS-80's, Commodore's, and so on. However, an enterprising school principal might be able to count a twenty-user Sun or Plexus as a computer, and thus be able to provide perhaps twenty times the computing ability as another school that bought a single Apple II.

Further, this disparity could alter the formula which is designed to eliminate disparity in the schools with the "one unit of hardware per student".

Our suggestion made to the bill's authors has been to redefine "computer hardware" to incorporate the concept of a workstation to a multi-user system as a unit.

3. What is a Robot?

There are a number of bills before the United States Congress which attempt to develop research and development in robotics.

Three examples are HR 4046, "The National Robot and Automated Manufacturing System Leasing Act of 1983", HR 4047, "The Robot and Automated Manufacturing Systems Research and Education Act of 1983", and HR 4048, "Bill to Amend the Internal Revenue Code [23]-[25]. All of these bills are sponsored by Congressman Fuqua (D -Florida).

These bills would show some forethought in setting the groundwork for a rapidly developing robotics industry. However, they define a robot as "a programmable (or multifunction) manipulator designed to move material, parts, tools, or special devices through variable programmed motions for the performance of a variety of tasks" [25].

In this case, the proper way to proceed is not clear to the authors. However, it would seem arguable that any machine with a variety of switch settings would satisfy the definition --- an automobile? a washing machine? a digital watch? The changing switch settings would satisfy the test of programming or reprogramming in the absence of any concrete definition (not present in the aforementioned bills) of what constitutes programming.

4. Another Definition of a Computer

There are numerous bills, referred to above, before the United States Congress on the subject of "computer fraud" or "computer crime". As examples are cited HR 1092, (Nelson, D-Florida), HR 4259, "A Bill to establish the Computer security Research Program and the Interagency Committee on Computer Crime and Abuse", (Mica, D-Florida), and HR 4384, "The Computer Fraud Prevention Act of 1983", (Mica, D-Florida) [26]-[28].

All of these bills (and several others), have a definition of "computer" that raises some questions. In addition, these bills address the electronic corruption of information in a way that also raises questions.

The definition of a "computer" provided is: "an electronic, magnetic, optical, hydraulic, organic, or other high speed data processing device or system performing logical, arithmetic, or storage functions, and includes any property, data storage facility, or communications facility directly related to or operating in conjunction with such device or system, but such term does not include an automated typewriter or typesetter, or a portable hand-held calculator"

The offence created (with a maximum penalty of \$50,000 or five years) is an intentional and unauthorized act which "damages a ... computer; or ... causes or attempts to cause the withholding or denial of the use of a ... computer, or a computer program or stored information relating to a ... computer".

The definition of a computer seems to err, perhaps on the side of caution. Is a non-hand-held portable calculator thus a computer?

The definition of the offence seems to leave open the possibility of being able to alter data without being held liable under this section, as altering data does not withhold or deny the use of a computer.

5. The British Data Protection Bill

An advantage in studying the Data Protection Bill [13] through its parliamentary debates in the House of Lords and the House of Commons is that first, a number of computer professionals were, in fact, involved in the debate; and, second, many of these problems described herein were grappled with not completely successfully. Here is an excerpt from the debate on the difference between "information" and "data":

Mr. Baker: "... my worries about the Bill relate principally to businesses, especially small businesses ... According to the Bill ... 'data' means information recorded in a

form in which it can be processed by equipment operating automatically in response to instructions given for that purpose ... that is extremely wide ... the Bill will cover information held on a computer as well as word processors [and] microfilm equipment

Mr. Smith: "Is he right in saying that the Bill extends to word processors ... Word processors process words, not data ..." [12, p. 308].

This excerpt illustrates another difficulty in dealing with definitions. If data is information "recorded in a form in which it can be processed by equipment operating automatically", then any typed piece of paper must be data, since it can be processed by an optical reader; on the other hand, the entire thrust of the debate, as referred to above, was over the exclusion of manual files from the requirement to be registered.

In conclusion, these items may seem on the one hand hair-splitting; but, it is to be remembered, that the practice of our profession may be greatly affected by the nature of legislation brought forward. And it is unthinkable that such legislation could be passed without the informed views of computer professionals providing a measure of consent to the "body politic" in its deliberations.

REFERENCES

- [1] Bill C-19, "An Act to Amend the Criminal Code", House of Commons of Canada, 32nd Parliament, Hon Mark MacGuigan, First Reading, February 7, 1984.
- [2] Regina v. McLaughlin, 113 Dominion Law Reports, 1980, p. 386
- [3] Bill C-647, Private Member's Bill, 32nd Parliament, Mr Perrin Beatty
- [4] Bill C-628, Private Member's Bill, 32nd Parliament, Mr Gordon Taylor
- [5] "Trade and Technology It's Canada's Move", Rowland Frazee, Royal Bank of Canada, 1983
- [6] "Traded Computer Services", Rodney DeC Gray, Royal Bank of Canada, 1983.
- [7] Final Report, Subcommittee on Computer Crime of the Standing Committee on Justice and Legal Affairs, Ottawa, June 1983.
- [8] Letter, Hon Roland Penner, Attorney-General of Manitoba, Feb 14, 1984
- [9] Letter, Graham Walker, Legislative Counsel of Nova Scotia, Feb. 20, 1984
- [10] "Computer and Communications Security and Privacy Hearings", United States House of Representatives Committee on Science and Technology, 1984, 346 pp.

[11] "Computer Security", Louise Becker, Congressional Research Service, Report 83-135, Washington, 1983

[12] "Computer Crime and Security", Louise Becker, Congressional Research Service, #IB80047, Washington, 1984

[13] Hansard, House of Commons, Great Britain, 11 April 1983, pp. 292-330.

[14] "Testimony of David H. Flaherty", Hearings of the Subcommittee on Computer Crime of the Standing Committee on Justice and Legal Affairs, Appendix, Issue 5, Ottawa, May 3, 1983

[16] "The Cryptography Controversy", R. H. Cooper, Conflict Quarterly, Spring 1981, pp. 21-24.

[17] "Accreditation Update", CIPS Review, Sept.-Oct. 1983, p 19

[18] Plenary Address, Seymour Papert, ACM '83, October 25, 1983

[20] Proc. of the Workshop on Artificial Intelligence, Science Council of Canada, Ottawa, August 1983

[21] "Programming Language Concepts", C. Ghezzi and M. Jazayeri, Wiley, New York, 1982.

[22] HR 3750, United States 98th Congress, Mr. Wirth of Colorado

[23] HR 4046, United States 98th Congress, Mr. Fuqua of Florida

[24] HR 4047, United States 98th Congress, Mr. Fuqua of Florida

[25] HR 4048, United States 98th Congress, Mr. Fuqua of Florida.

[26] HR 1092, United States 98th Congress, Mr. Nelson of Florida.

[27] HR 4259, United States 98th Congress, Mr. Mica of Florida.

[28] HR 4384, United States 98th Congress, Mr. Mica of Florida

Appendix A

Summary of Pending

Computer-Related Legislation

Canada

Computer Crime

Bill C-19 (Mr. MacGuigan)

United States

Computer Crime

HR 1092 (Nelson, D-Fla)
HR 3075 (Wyden, D-Ore)

HR 4259 (Mica, D-Fla)
HR 4301 (Coughlin, R-Pa)
HR 4384 (Mica, D-Fla)
S 1733 (Trible, R-Va)
S 1920 (Tsongas, D-Mass)
S 2270 (Cohen, R-Maine)

Computer Literacy/ Computers in the

HR 91 (Donnelly, D-Mass)
HR 659 (Perkins, D-Ky)
HR 701 (Stark, D-Cal)
HR 2417 (Wright, D-Tex)
HR 2531 (Gingrich, R-Cal)
HR 3750 (Wirth, D-Col)
S 1093 (Dodd, D-Conn)
S 1194 (Danforth, R-Mo)
S 1195 (Bentsen, D-Tex)
S 1285 (Hatch, R-Utah)
S 1849 (Lautenberg, D-NJ)

Computer Science Training/ Higher Ed

HR 1310 (Perkins, D-Ky)
HR 1699 (Perkins, D-Ky)
HR 2483 (LaFalce, D-NY)
HR 3095 (Shannon, D-Mass)
HR 3098 (Stark, D-Cal)
HR 3280 (Gunderson, R-Wisc)
HR 4244 (Jenkins, D-Ga)
HR 4475 (Shannon, D-Mass)
S 530 (Pell, D-RI)
S 874 (Kennedy, D-Mass)
S 1055 (Quayle, R-Ind)
S 1087 (Hatch, R-Utah)
S 1869 (Dodd, D-Conn)
S 2165 (Danforth, R-Mo)

National Computer Institute

S 2204 (Heflin, D-Ala)

National Educational Software Corpor

HR 4228 (Skelton, D-Mo)
HR 4628 (Gore, D-Tenn)

Office Machine Equipment

HR 1159 (Alexander, D-Ark)
S 286 (Exon, D-Neb)

Robotics Research and Development

HR 1036 (Hawkins, D-Cal)
HR 3485 (Hawkins, D-Cal)
HR 4046 (Fuqua, D-Fla)
HR 4047 (Fuqua, D-Fla)
HR 4048 (Fuqua, D-Fla)

Suspension of Duty on Computer Parts

HR 1410 (St Germain, D-RI)

Unauthorized Copying of Chips and Ma

HR 1028 (Edwards, D-Cal)
S 1201 (Mathias, R-Md)

Great Britain

Privacy of Information
Data Protection Bill

CA1

Z2

- C52

DOCUMENT : 870-123/006

Traduction du Secrétariat

CONFÉRENCE INTERPROVINCIALE SUR LA PROTECTION
DES RENSEIGNEMENTS PERSONNELS :
MESURES POUR 1984 (COLLOQUE)

Raisons pour lesquelles les informaticiens
et le secteur de l'informatique doivent
chercher à influencer sur les projets de loi futurs

(Extraits des comptes rendus des séances de 1984
de l'Association canadienne de l'informatique)

Rodney H. Cooper,
Département de l'informatique, Université du Nouveau-Brunswick
et Wayne Patterson,
Département de mathématique, de physique et d'informatique
Université de Moncton



Toronto (Ontario)
Les 23 et 24 mai 1984

Raisons pour lesquelles les informaticiens
et le secteur de l'informatique doivent
chercher à influencer sur les projets de loi futurs

Rodney H. Cooper* et Wayne Patterson**

* Département de l'informatique, Université du Nouveau-Brunswick, Fredericton

** Département de mathématique, de physique et d'informatique, Université de Moncton

RÉSUMÉ --- L'article est divisé en trois sections : Dans la première section, les auteurs examinent les projets de loi actuels au Canada, aux États-Unis, et en Grande-Bretagne qui touchent l'informatique. Dans la deuxième section, on étudie la possibilité de projets de loi futurs au Canada. Dans la dernière section, on donne quelques exemples des dangers qui peuvent se produire si des lois que les informaticiens n'ont pas bien scrutées sont adoptées.

"Perspectives d'inquiétudes et d'espoirs" --- Cette expression décrit bien ce que les informaticiens doivent ressentir devant l'intervention récente du facteur des politiques publiques dans notre profession.

La profession peut fonder de grands espoirs sur le fait que les divers gouvernements au Canada et à l'étranger commencent à s'intéresser à des aspects qui revêtent une importance considérable pour notre profession et l'ensemble de la société. Cette activité sur le plan législatif révèle manifestement qu'on se rend généralement compte de l'influence de notre profession et qu'il est temps de s'attaquer aux lois touchant l'informatique.

L'objectif du présent document comporte trois volets. Le premier consistera en une analyse des projets de loi actuels au niveau du gouvernement du Canada et des provinces canadiennes ainsi qu'aux États-Unis et en Grande-Bretagne.

Le deuxième examinera les secteurs d'intérêt législatif probable tandis que le troisième et dernier volet fera ressortir plusieurs inquiétudes du secteur de l'informatique. Nous soutiendrons que les informaticiens doivent participer beaucoup plus étroitement à l'élaboration des politiques publiques qui les concernent parce que même les principes législatifs les plus louables peuvent avoir des conséquences malheureuses lorsque les projets de loi négligent de faire entrer en ligne de compte les considérations techniques pertinentes. Nous étayerons notre position en citant plusieurs exemples et nous ferons état de certaines précautions qu'il y aurait lieu de prendre.

A. Les projets de loi actuels

Ce volet sera divisé en cinq parties, soit le Canada, les provinces, les États-Unis, les divers États américains et la Grande-Bretagne.

Canada

Le projet de loi C-19 (1) est le seul à avoir été déposé à la Chambre des communes. Il créerait deux nouvelles infractions dans le Code criminel. La première serait l'utilisation non autorisée d'un ordinateur : "Quiconque, malhonnêtement... a) directement ou indirectement, obtient des services d'ordinateur, b) au moyen d'un dispositif électromagnétique, acoustique, mécanique ou autre, directement ou indirectement, intercepte ou fait intercepter toute fonction d'un ordinateur, c) directement ou indirectement, utilise ou fait utiliser un ordinateur dans l'intention de commettre une infraction... est coupable d'un acte criminel et passible d'un emprisonnement maximal de dix ans ou d'une infraction punissable par procédure sommaire (1)."

La deuxième infraction est le "méfait concernant les données" : "Commet un méfait quiconque, volontairement, a) détruit ou modifie des données; b) dépouille les données de leur sens, les rend inutiles ou inopérantes; c) empêche, interrompt ou gêne l'emploi légitime des données; ou d) empêche, interrompt ou gêne une personne dans l'emploi légitime des données ou refuse l'accès aux données à une personne qui y a droit (1)." L'auteur de l'infraction de méfait concernant les données est également passible de dix de prison ou de condamnation par la procédure sommaire. Au moment de la rédaction du présent document, le projet de loi en question (déposé le 7 février 1984) n'avait pas été soumis à l'examen en comité. C'est donc dire que la plus importante étude du projet de loi n'avait pas encore eu lieu. Le secteur de l'informatique a néanmoins vanté les mérites de certains articles du projet de loi C-19.

Il été jusqu'à présent extrêmement difficile, voire impossible, pour tout propriétaire d'un système d'ordinateurs d'obtenir réparation juridique lorsque des usagers non autorisés obtiennent accès au système grâce à des dispositifs électroniques. La cause la plus célèbre soumise aux tribunaux canadiens et celle de La Reine c. McLaughlin (2) dans laquelle une condamnation initiale de vol d'information a été renversée en appel.

Il est à souhaiter que les dispositions actuelles, sous réserve de l'avertissement contenu dans la troisième partie du présent document, fourniront de meilleurs motifs de poursuite.

En plus du projet de loi C-19, des projets de loi d'intérêt privé portant sur la sécurité de l'informatique ont également été déposés à la 32^e législature du Parlement (3), (4).

En outre, il existe dans plusieurs ministères fédéraux des groupes de travail qui étudient les secteurs dans lesquels il peut être possible de légiférer. Il s'agit notamment de l'échange transfrontière de données, de la loi sur le droit d'auteur et de la réaction canadienne aux projets s'insérant dans le cadre de la cinquième génération d'ordinateurs. De plus, le Comité permanent de la justice et des affaires juridiques de la Chambre des communes a tenu, l'an dernier, une audience et publié un rapport sur la fraude informatique et d'autres questions.

Il s'agit des documents 5, 6 et 7 de la bibliographie.

2. Provinces canadiennes

Les auteurs ont récemment écrit à tous les procureurs généraux canadiens pour connaître les projets de loi actuels dans ce domaine. Au moment de la rédaction du présent rapport, seuls la Nouvelle-Écosse et le Manitoba avaient répondu qu'ils avaient un projet de loi dans le secteur de l'informatique. Le procureur général du Manitoba a précisé qu'une loi sur la liberté de l'information étant en voie d'élaboration (8).

Voici un extrait de la réponse de la Nouvelle-Écosse:

(traduction)

"Notre loi de 1977 sur la liberté de l'information (Freedom of Information Act), c. 10, S.N.-É., comporte une disposition d'application générale concernant la protection des renseignements contenus dans les dossiers d'un ministère (provincial)... De plus, la législature a adopté en vertu de notre Consumer Reporting Act de 1973, c.4, S.N.-É. des restrictions concernant les renseignements qui peuvent être versés au dossier d'un consommateur, l'utilisation qui peut en être faite et la divulgation de ces renseignements. Le mot "dossier" est défini de sorte qu'il s'applique à toutes les formes et à toutes les méthodes d'emmagasiner de l'information." (9)

3. États-Unis

Il y a une prolifération de projets de loi touchant l'informatique aux États-Unis et cela est dû en grande partie à l'existence même du système de Congrès. De fait, le Congrès a déjà été saisi d'au moins 46 projets de loi relatifs à l'informatique. Des lois existent dans les principales catégories suivantes : les connaissances en informatique, la fraude informatique, la sécurité de l'informatique dans la petite entreprise, la sécurité et la protection de la recherche en informatique, la recherche en robotique et la fabrication dans ce domaine, la protection contre la reproduction de masques de silicone, les tarifs et l'unité de disques de l'axe.

Un tableau complet de ces lois est présenté à l'annexe A. Des conversations avec des législateurs et leurs aides à Washington ont révélé qu'il est fort probable que soit adopté un projet de loi sur "les connaissances en informatique". Il existe deux tendances contraires dans ce domaine.

La première (projet de loi Stark ou Apple) prévoit des allègements fiscaux pour les fabricants d'ordinateurs qui fournissent leur produit à des écoles ou à d'autres établissements à but non lucratif. L'autre tendance (projet de loi Wirth) prévoit l'affectation de crédits aux programmes d'informatique scolaire aux fins de l'achat de matériel et de logiciel, et de la formation d'enseignants.

L'autre vaste secteur de législation qui a suscité beaucoup de discussions est celui de la sécurité de l'informatique. D'importantes audiences ont eu lieu (10) le 26 septembre 1983 et du 17 au 24 octobre de la même année sur cette question. Toutefois, en raison de l'opposition que manifestent actuellement le ministère de la Justice et le FBI, il est peu probable que les divers projets de loi dans ce domaine aillent de l'avant.

Il est intéressant de comparer la réaction des informaticiens canadiens et américains aux projets de loi sur la fraude informatique. Au Canada, ils semblent appuyer fortement le projet de loi tandis qu'aux États-Unis, il y a soit un intérêt marginal ou une opposition tacite (11).

Le Congrès s'est également penché sur d'autres aspects sans incidence législative, notamment l'abolition du monopole en matière d'installations de télécommunications (la fragmentation des sociétés de téléphone) et la fabrication de superordinateurs.

4. Les États

Au moment de la rédaction du présent rapport, vingt États avaient adopté une forme quelconque de projet de loi sur la fraude de informatique, il s'agit de l'Arizona, de la Californie, du Colorado, du Delaware, de la Floride, de la Georgie, de l'Illinois, du Massachusetts, du Michigan, du Minnesota, du Montana, du Nouveau Mexique, de la Caroline du Nord, de l'Ohio, du Rhode Island, du Dakota du Sud, du Tennessee, de l'Utah, de la Virginie et du Wisconsin (12).

De plus, la Californie a adopté sa propre version du projet de loi baptisé "Apple" et la Société Apple a par conséquent fait don d'ordinateurs (à raison d'un par école).

5. Grande-Bretagne

Le Parlement de Grande-Bretagne n'a été saisi que d'un seul projet de loi dans ce domaine. Il s'agit du Data Protection Bill (13). Le projet de loi en question a obtenu (à deux reprises) la

sanction de Chambre des lords en 1983 et il se trouve en ce moment devant la Chambre des communes.

L'objectif du projet de loi est de mettre la vie privé des individus à l'abri des intrusions en protégeant les renseignements personnels contenus dans les fichiers de données des secteurs privés et publics.

En bref, le projet de loi obligera les propriétaires de fichiers de données à se procurer un permis. Le processus d'octroi de permis comportera vraisemblablement des exigences en ce qui a trait à la sécurité du système d'ordinateurs, au respect du droit de l'individu à sa vie privé et à l'accès à donner à l'individu.

Le point de vue du gouvernement est que le projet de loi est indispensable en raison de l'augmentation incroyable des renseignements contenus dans les ordinateurs. L'opposition a pour sa part soutenu que le projet de loi n'a été mis de l'avant que pour répondre à une exigence de la Communauté économique européenne touchant la protection des données et que l'industrie britannique pourrait être désavantagée dans ses relations commerciales avec l'Europe si on ne se dote pas d'un projet de loi dans ce domaine.

Les principaux points de conflit dans le débat sur le projet de loi ont été le fait (1) que le projet de loi ne vise que les dossiers informatisés et non les dossiers manuels; (2) que c'est une personne et non un organisme qui est chargée de faire respecter la loi; (3) qu'une exemption est prévue pour certaines catégories de renseignements gouvernementaux; et (4) que soient définies des méthodes devant servir à mettre le public au courant des renseignements que possèdent les banques de données à leur sujet.

B. Secteurs dans lesquels il est possible de légiférer

Les ordinateurs et la technologie de la micro-électronique auront des incidences énormes sur la société et les incidences iront manifestement en s'amplifiant.

Dans toute société, les conflits s'accroissent inévitablement lorsqu'une série de facteurs touche de plus en plus de membres. Dans une société démocratique, les institutions de biens publics tels que les gouvernements doivent mettre au point des méthodes pour prévoir et contrôler ces conflits.

Par essence même, les gouvernements agissent lentement et avec circonspection. C'est pourquoi, ils n'ont toujours pas réglé de nombreux problèmes sociaux soulevés par l'adoption de nouvelles technologies. Le présent article s'efforcera de mettre en relief certains de ces secteurs de conflits réels et potentiels.

La vie privée

Nous avons délibérément placé cet aspect en tête de liste. Un certain nombre de sondages (14) ont révélé que le public canadien craint surtout que les nouvelles technologies ne favorisent des intrusions dans la vie privée (plutôt que la perte d'un emploi qui est habituellement considérée comme la principale crainte par les médias).

Au Canada, il n'existe pratiquement aucune loi dont l'objet précis est de mettre les citoyens à l'abri des intrusions dans leur vie privée rendues possibles grâce à la quantité de données de plus en plus impressionnante emmagasinée dans les ordinateurs.

Toutefois, certaines lois et certains règlements régissent l'utilisation qui est faite de l'information au sein même du gouvernement. Par exemple, il est interdit à un ministère d'utiliser les données d'un autre. (La Commission l'assurance-chômage ne peut, par exemple, examiner régulièrement les dossiers de Revenu Canada pour voir si les bénéficiaires ont un emploi caché.)

Il est toutefois fort peu probable que les Canadiens trouvent un réconfort dans les principes qui existaient avant l'arrivée des ordinateurs.

Supposons par exemple que la Commission d'assurance-chômage et Revenu Canada décident d'utiliser le même système de gestion des bases de données pour combiner leurs comptes, sauver de l'espace, ménager les machines et réaliser des économies. Doit-on leur permettre de prendre une pareille décision? Constituerait-elle une violation inhérente du droit à la vie privée? Qu'en serait-il si la technologie du système de gestion des bases de données était tellement avancée qu'il serait, par exemple, plus onéreux de consulter les dossiers d'un autre ministère que d'entrer par effraction dans ses bureaux (ou de forcer l'accès à ses ordinateurs)?

Quoi qu'il en soit, il semble n'exister à l'heure actuelle, au gouvernement fédéral et parmi tous les gouvernements provinciaux, aucune norme de protection de la vie privée ou contre les dangers de l'ordinateur. La première étape qui s'impose consiste donc à établir de pareilles normes pour éviter les abus gouvernementaux et les abus résultant d'interventions extérieures.

À tout le moins, il faudrait rédiger une loi rendant obligatoire l'encryptage de toutes les données jugées de caractère confidentiel et préciser que toutes les données concernant les particuliers sont confidentielles (16).

Pour cette raison, il semble nécessaire d'établir des modalités d'élaboration d'une norme canadienne d'encryptage des données.

Les citoyens s'inquiètent non seulement des données recueillies par les gouvernements mais également de celles qui sont recueillies par le secteur privé.

Des normes analogues à celles dont il vient d'être question doivent donc également être adoptées par les banques, les établissements de crédit, les sociétés d'assurance et le secteur de la santé ou leur être imposées par la loi. Il est toujours préférable qu'un secteur industriel se réglemente lui-même. Néanmoins, la loi devrait comporter une disposition exigeant que les normes industrielles soient tout au moins aussi rigoureuses que les normes que le gouvernement s'impose.

La fraude informatique

Le vol au moyen d'ordinateurs est devenu une grosse affaire. La fraude informatique se retrouve partout. Elle est difficile à déceler et reste souvent impunie. Il y a l'exemple insignifiant d'un étudiant de collège qui copie le programme de quelqu'un d'autre, celui du "vandale" qui détruit des dossiers de valeur et, finalement, celui du voleur professionnel qui modifie des comptes. La cause canadienne type La Reine c. McLaughlin (2) a révélé à quel point il est difficile d'intenter des poursuites.

Comme nous l'avons déjà dit, le ministre de la Justice du Canada, l'honorable Mark MacGuigan, a récemment déposé un projet de loi (1) qui ferait un crime, rendant son auteur passible d'un emprisonnement maximal de 10 ans, de l'utilisation non autorisée d'un ordinateur.

Un des problèmes que posera le projet de loi sera sa mise en application. Comme c'est le cas pour une bonne part du Code criminel du Canada, il appartient à l'administration fédérale de définir l'infraction mais aux provinces d'effectuer la mise en application.

À l'heure actuelle, les organismes chargés de la mise en application des lois provinciales sont peu spécialisés en matière de détection des infractions touchant les ordinateurs et de poursuites s'y rapportant.

Le droit d'auteur

Le droit d'auteur est un principe ancien dans le système juridique britannique. Au cours des dernières années, il a subi l'assaut de la technologie qui en a étendu le sens jusqu'à la limite.

L'inquiétude suscitée par le droit d'auteur s'est accentuée il y a quelques années lorsque l'utilisation de photocopieur s'est répandue. Dans quelles conditions est-il légal, le cas échéant, de reproduire un livre?

La question a pris encore plus d'importance avec la mise en marché, il y a une quinzaine d'années, de dispositifs d'enregistrement à prix populaires et cette importance s'est accrue avec l'arrivée des magnétoscopes.

La presse a subi le même phénomène fondamental. Il est important et légitime pour ces techniques d'utiliser des dispositifs de reproduction économiques. Lorsque de tels dispositifs existent, il est logique de s'en servir.

Avant de légiférer davantage dans le domaine du droit d'auteur, il faudrait répondre à deux questions :

Existe-t-il des épreuves ou des normes permettant de déterminer dans quelles circonstances il peut être légitime de reproduire du logiciel? (La réponse sera probablement affirmative mais il n'y a risque d'effacement accidentel des données emmagasinées que si on utilise des disques).

Deuxièmement, existe-t-il des normes quantitatives pour déterminer ce qui constitue un plagiat (par opposition à une simple reproduction)? Cette question est manifestement beaucoup plus complexe dans le cas du logiciel.

Les experts en détection de fraudes touchant l'art ou en vols dans le secteur littéraire peuvent la plupart du temps dire si un auteur, un peintre ou un compositeur a plagié un autre mais il peut être extrêmement difficile d'obtenir le même résultat dans le cas d'un programme en suivant une démarche publique.

Signalons que le ministère de la Justice du Canada a chargé un groupe d'étude d'examiner cette question.

L'échange international de données

L'échange de données à l'échelle transnationale est un autre secteur dans lequel il est possible de légiférer.

Il est normal pour le Canada de se demander si l'échange incontrôlé de données par delà les frontières est dans l'intérêt national ou public.

Le ministère des Communications s'est penché sur cette question.

À l'heure actuelle, bon nombre d'industries comptent sur l'emmagasinage et le traitement de données par des ordinateurs situés à l'étranger.

La première question à laquelle il faut répondre est la suivante: Y a-t-il un intérêt national stratégique à veiller à ce que les données proprement "canadiennes" soient, de quelque façon, sous

contrôle canadien. Par exemple, s'il existait une norme de sécurité canadienne pourrait-on ou devrait-on exiger qu'elle s'applique aux données emmagasinées par des ordinateurs situés à l'étranger?

La deuxième question est d'ordre économique. Doit-on laisser dans des ordinateurs situés à l'étranger des données recueillies au Canada? Si la réponse est affirmative, on peut facilement entrevoir le jour où il existera "des paradis de l'informatique" tout comme certains pays sont devenus des "paradis fiscaux".

Ce deuxième point soulève évidemment la question de l'opposition entre le libre échange et le protectionnisme.

La dernière question connexe a trait à l'importance qu'accordent les gouvernements aux données informatisées recueillies et emmagasinées à l'étranger mais qui sont utilisées par des Canadiens. Des exemples courants sont les banques de données utilisant la technique en ligne, notamment Dialog, BRS et CompuServe.

La Banque Royale du Canada a effectué une importante étude sur cette question (5), (6).

Certification et accréditation professionnelles

Au fur et à mesure que la profession fera sa place, la question de la certification professionnelle suscitera l'intérêt des législateurs.

Si on suit le même cheminement que pour les autres professions, cette certification relèvera des administrations provinciales. Les associations du barreau, les sociétés médicales et les associations d'ingénieurs professionnels sont toutes régies par des règlements des législatures provinciales auxquelles elles doivent également leurs pouvoirs, même si ces diverses sociétés sont souvent groupées en associations nationales.

Les lois en vertu desquelles les membres des autres professions obtiennent leur certification prévoient un processus d'accréditation des programmes menant aux diplômes.

L'Association canadienne de l'informatique a lancé un programme d'accréditation de cours universitaires en informatique (17). Le Canada est donc en avance sur les États-Unis où l'ACM étudie la question de l'accréditation mais n'a encore mis en oeuvre aucun projet s'y rapportant.

C'est à l'ensemble du secteur de l'informatique qu'il appartient de décider s'il est dans son intérêt d'obtenir un statut professionnel par la voie législative. L'autre solution est que les gouvernements décident que la certification et la réglementation sont nécessaires et qu'ils les imposent à la profession.

Les ordinateurs dans les écoles

Les gouvernements provinciaux s'interrogent également sur la place des ordinateurs dans les programmes scolaires et le gouvernement fédéral accorde à cet aspect plus qu'un intérêt marginal.

Les ministères provinciaux de l'Éducation ont décidé de doter les écoles d'ordinateurs de toute urgence. En règle générale, cette orientation fut prise sans l'adoption d'aucune loi.

Les opinions des informaticiens sur l'utilisation des ordinateurs dans les écoles sont extrêmement variées. Elles se situent entre le principe de Seymour Papert selon lequel les "ordinateurs sont des crayons" (18) et la conviction qu'ont de nombreux informaticiens que l'informatique ne doit aucunement être enseignée au niveau précollégial.

De nombreux aspects de l'utilisation des ordinateurs dans les écoles peuvent être réglés en légiférant. Par exemple, les provinces pourraient ordonner l'enseignement de l'informatique ou "de connaissances en informatique".

Les provinces pourraient également fixer des normes de compétence pour les professeurs qui enseignent des cours se rapportant à l'informatique, ce qui ne se fait pas à l'heure actuelle.

Le code d'éthique en informatique

L'an dernier, le Comité permanent de la justice et des questions juridiques de la Chambre des communes (7) a présenté un rapport sur un certain nombre d'aspects se rapportant à l'utililisation des ordinateurs.

Une des recommandations était que des cours sur l'éthique en informatique soient enseignés aux niveaux scolaire et universitaire.

Cette question rejoint manifestement les deux points précédents mais il en est question en raison de l'allusion précise du Comité permanent.

Le branchement clandestin

Il existe à l'heure actuelle au Canada beaucoup de dispositions législatives sur le branchement clandestin.

Il faut toutefois se demander si les lois actuelles ont une portée assez large pour englober le branchement clandestin sur des lignes de transmission de données.

Soulignons que nous n'avons traité que de quelques-uns des aspects qui pourraient faire l'objet d'un examen législatif au cours des prochains mois ou des prochaines années. En terminant, en voici d'autres auxquels il faudrait réfléchir : la définition de ce qu'est une lettre et les conséquences de cette définition pour Postes Canada et le courrier électronique; les lois concernant le déplacement d'emplois et le recyclage; l'adoption par le Canada de la technique de la cinquième génération (20); les lois sur l'utilisation des robots dans l'industrie.

C. Les responsabilités des informaticiens

Une analyse minutieuse de presque toutes les lois dont il a été question à la partie A révèle pourquoi il est extrêmement important que le secteur de l'informatique et les informaticiens contrôlent l'élaboration de toutes les lois qui auront une incidence sur la collectivité et qu'ils participent à ce processus d'élaboration.

Les lois dans le secteur de l'informatique exigent une connaissance approfondie de questions techniques que souvent seuls les professionnels possèdent.

Par conséquent, il existe un grand danger que des lois élaborées par d'autres que des informaticiens ne comportent des échappatoires ou n'entraînent des résultats inattendus. Nous donnerons cinq exemples tirés des projets de loi mentionnés à la partie A pour illustrer ce point.

1. La définition d'un programme d'ordinateur

Le projet de loi C-19 de la Chambre des communes du Canada (1), dont il a déjà été question, contient des dispositions établissant la "fraude informatique". La définition suivante est donnée de l'expression "programme d'ordinateur" dans le projet de loi : "Un ensemble de données qui représentent des instructions ou des relevés et qui, lorsque traitées par l'ordinateur, lui font remplir une fonction." Il faut examiner très attentivement cette définition. Une définition simpliste du langage des programmes est justement que celui-ci consiste en une série d'"instructions" ou de "relevés" qui, exécutés en ordre, font qu'une certaine tâche est exécutée. Cette forme de langage de programme correspond à la définition que Neumann donne d'un ordinateur.

Toutefois, il est également vrai que de nombreux langages d'ordinateur ne comportent ni instructions ni relevés. Les langages fondés sur le modèle Neumann sont souvent baptisés "langages impératifs" (21). Il y a toutefois une autre catégorie de langages, soit les langages "fonctionnels" ou "d'application". Dans ces langages, le programme n'est pas une série de relevés mais plutôt une fonction. On obtient l'exécution du programme en appliquant la fonction à ses arguments. LISP, Prolog et, d'après certains auteurs, APL sont des langages d'application.

Le danger que pose l'utilisation de la définition déjà donnée pour les "programmes d'ordinateur" est donc évident. On peut facilement imaginer que la destruction d'un programme LISP, ou même d'un projet complet d'intelligence artificielle, ne soit pas visée par le Code criminel parce que la défense serait en mesure de prouver que les programmes LISP ne sont pas des "programmes d'ordinateur" d'après la définition contenue dans le projet de loi C-19.

La solution dans ce cas est cependant facile puisqu'un examen du projet de loi révèle qu'on peut en modifier le libellé sans nécessairement traiter de programmes d'ordinateur (ce qui établit une distinction entre les programmes et les autres genres de données). Cette solution temporaire ne serait toutefois pas valable lorsqu'il faut définir les programmes d'ordinateur aux fins de la loi sur le droit d'auteur.

2. Un ordinateur, un étudiant?

L'important projet de loi HR 3750 (Wirth, D-Colorado) a été déposé au Congrès des États-Unis. Il s'agit de "The Computer Literacy Act of 1983" (loi de 1983 sur les connaissances en informatique) dont l'objectif est de favoriser l'acquisition de connaissances en informatique par les étudiants et les professeurs aux niveaux élémentaire et secondaire (22). Une disposition du projet de loi prévoit que des crédits seront mis à la disposition des districts scolaires aux fins de l'achat d'ordinateurs et de logiciels et de la formation des enseignants.

Le projet de loi prévoit en outre l'affectation de crédits en fonction de l'importance des besoins. C'est-à-dire que les écoles qui possèdent le moins d'ordinateurs en fonction du nombre d'étudiants seront privilégiées et qu'aucune aide ne sera accordée à aucune école qui aura au moins l'équivalent d'une unité de matériel pour chaque groupe de 30 enfants.

"Matériel" est ensuite défini en précisant qu'un ordinateur égale une unité de matériel. Les auteurs du projet de loi n'ont pas tenu compte du fait qu'un réseau à usagers multiples offre des possibilités intéressantes en matière d'achats scolaires. La raison en est sans doute que presque toutes les discussions touchant les ordinateurs scolaires portaient sur des micro-ordinateurs à un seul usager tels que les Apple II, les TRS-80, les Commodore Pet's et autres. Toutefois, un directeur d'école débrouillard pourrait considérer un Sun ou un Plexus à vingt usagers comme un seul ordinateur et être en mesure d'offrir jusqu'à vingt fois plus d'accès aux services informatisés qu'une autre école qui achèterait un seul Apple II. Qui plus est, la différence risque de fausser la formule destinée à combler l'écart avec les écoles qui possèdent le moins de matériel par étudiant.

Notre suggestion à l'auteur du projet de loi a été qu'il redéfinisse le terme matériel ou ordinateur de façon à y incorporer la définition d'un poste de travail d'un réseau à usagers multiples comme une unité.

3. Qu'est-ce qu'un robot?

Un certain nombre de projets de loi déposés au Congrès des États-Unis visent à favoriser la recherche et le développement en robotique.

Trois de ces projets de loi sont : HR 4046, "The National Robot and Automated Manufacturing Systems Leasing Act of 1983"; HR 4047, "The Robotics and Automated Manufacturing Systems Research and Education Act of 1983"; et HR 4048, "A Bill to Amend the Internal Revenue Code" (23)-(25). Tous ces projets de loi sont parrainés par le même membre du Congrès, M. Fuqua (D-Floride).

Ces projets de loi traduisent une certaine prévoyance en matière d'établissement des fondements d'une industrie de robotique en plein essor. Toutefois, dans tous les cas, un robot est défini comme un dispositif de manipulation programmable aux fonctions multiples destiné à déplacer des matériaux, des pièces, des outils ou des mécanismes spécialisés en exécutant des gestes programmés (sic) et variables afin d'accomplir diverses tâches (25).

Les auteurs semblent toujours à la recherche d'une solution à ce problème. Il semble toutefois y avoir danger qu'on puisse soutenir que n'importe quelle machine munie de différents réglages d'interrupteurs répond à cette définition, par exemple une automobile, une lessiveuse, une montre à affichage numérique. En l'absence d'une définition précise (qui fait défaut dans les projets de loi en question) de ce qui constitue une programmation, le réglage des interrupteurs répondrait au critère de programmation ou de reprogrammation.

4. Autre définition d'un ordinateur

De nombreux projets de loi déposés devant le Congrès des États-Unis, et dont il a déjà été question, traitent de la "fraude informatique". Ce sont notamment les projets de loi HR 1092, (Nelson, D-Floride), HR 4259, "A Bill to establish the Computer security Research Program and the Interagency Committee on Computer Crime and Abuse", (Mica, D-Floride); et HR 4384, "The Computer Fraud Prevention Act of 1983", (Mica, D-Floride) (26)-(28).

Tous ces projets de loi (et plusieurs autres), donnent une définition d'"ordinateur" qui soulève certaines questions. La manière dont ces projets de loi traitent de l'altération électronique des données soulève elle aussi des questions.

La définition suivante est donnée d'un ordinateur: "(traduction) un dispositif où un système électronique, magnétique, optique hydraulique, organique ou autre de traitement des données à grande vitesse qui exécute des fonctions logiques, arithmétiques ou d'emmagasinement. La définition s'étend également à tout bien, toute installation d'entreposage de données ou installation de communications directement rattaché à ce dispositif ou à ce système ou fonctionnant avec lui, mais elle exclut les machines à écrire ou à composer automatiques ainsi que les calculatrices manuelles portatives."

L'infraction créée (pour laquelle la sanction maximale d'une amende de 50 000 \$ ou de 5 ans d'emprisonnement est prévue) consiste en un acte intentionnel et non autorisé qui "(traduction) endommage ... un ordinateur ou... a pour objet de refuser ou de chercher à interdire l'accès... à un ordinateur, à un programme d'ordinateur ou aux données informatisées emmagasinées".

La définition d'un ordinateur semble pécher par excès de prudence. Ainsi, peut-on dire qu'une calculatrice portative qui n'est pas de format de poche est un ordinateur?

La définition qui est donnée de l'infraction laisse planer la possibilité que des données soient modifiées sans entraîner aucune poursuite en vertu de l'article en question parce qu'en altérant des données on ne refuse ni interdit l'accès à un ordinateur.

5. Projet de loi britannique sur la protection des données

L'intérêt d'étudier l'évolution du projet de loi en question (13) au cours des débats parlementaires à la Chambre des lords et à la Chambre des communes réside dans le fait, en premier lieu, qu'un certain nombre d'informaticiens ont réellement participé au débat et, en deuxième lieu, que bon nombre de solutions apportées aux problèmes n'étaient pas entièrement satisfaisantes. Voici par exemple un extrait du débat sur la différence qui existe "information" et "donnée":

M. Baker "... (traduction) mes inquiétudes au sujet du projet de loi ont trait d'abord aux entreprises et surtout aux petites entreprises... le projet de loi définit... "données" comme des informations conservées dans une forme qui permet de les traiter en utilisant un dispositif automatique qui répond à des instructions en ce sens... Or, cette définition étant extrêmement vaste, le projet de loi englobera à la fois les renseignements en ordinateur, les machines de traitement de textes et les appareils à microfilms."

M. Smith: "(traduction) A-t-il raison d'affirmer que le projet de loi s'étendrait aux machines de traitement de textes ... Ces machines traitent des mots et non des données..." (12, p. 308).

Cet extrait illustre une autre difficulté que posent les définitions. Si les données sont des informations "conservées dans une forme qui permet de les traiter en utilisant un dispositif automatique" alors n'importe quel document dactylographié constitue également des données puisqu'il peut être traité au moyen d'un dispositif de lecture optique. Par contre, comme nous l'avons vu, tout le débat a porté essentiellement sur l'exclusion des dossiers manuels de l'exigence d'enregistrement.

En conclusion, il peut sembler que l'on cherche à couper les cheveux en quatre mais rappelons-nous que notre profession risque d'être grandement touchée par la teneur des projets de loi qui seront soumis. Il est impensable que ces projets de loi soient adoptés sans que le corps politique fasse appel à un certain consentement de la part des informaticiens compétents.

RÉFÉRENCES

- (1) Projet de loi C-19, "Loi modifiant le Code criminel", Chambre des communes du Canada, 32^e législature, l'honorable Mark MacGuigan, première lecture, le 7 février 1984.
- (2) La Reine c. McLaughlin, 113 Dominion Law Reports, 1980, p. 386.
- (3) Projet de loi C-667, projet de loi d'intérêt privé, 32^e législature, M. Perrin Beatty.
- (4) Projet de loi C-628, projet de loi d'intérêt privé, 32^e législature, M. Gordon Taylor.
- (5) "Trade and Technology : It's Canada's Move", Rowland Frazee, Banque Royale du Canada, 1983.
- (6) "Traded Computer Services", Rodney D & C Gray, Banque Royale du Canada, 1983.
- (7) Rapport final, Sous-comité sur la fraude informatique du Comité permanent de la justice et des questions juridiques, Ottawa, juin 1983.
- (8) Lettre de l'hon. Roland Penner, procureur général du Manitoba, le 14 février 1984.
- (9) Lettre de Graham Walker, conseiller législatif de la Nouvelle-Écosse, le 20 février 1984.
- (10) "Computer and Communications Security and Privacy Hearings", Comité sur la science et la technologie de la Chambre des représentants des É.-U., 1984 pages 546 et suivantes.

- (11) "Computer Security", Louise Becker, Congressional Research Service, Report 83-135, Washington, 1983.
- (12) "Computer Crime and Security", Louise Becker, Congressional Research Service, IB80047, Washington, 1984.
- (13) Hansard, Chambre des communes, Grande Bretagne, le 11 avril 1983, pages 292 à 330.
- (14) Témoignage de David Flaherty, audiences du Sous-comité sur la fraude informatique du Comité permanent de la justice et des questions juridiques, annexe, fascicule 5, le 3 mai 1983.
- (16) "The Cryptography Controversy", R. H. Cooper, Conflict Quarterly, printemps 1981, pages 21 à 24.
- (17) "Accreditation Update", CIPS Review, sept. - oct. 1983, p. 19.
- (18) Plenary Address, Seymour Papert, ACM '83, le 25 octobre 1983.
- (20) Procès-verbal de l'atelier sur l'intelligence artificielle, Conseil des sciences du Canada, Ottawa, août 1983.
- (21) Programming Language Concepts", C Chezzi et M. Jazayeri, Wiley, New York, 1982.
- (22) HR 3750, 98^e Congrès des É.-U., M. Wirth du Colorado.
- (23) HR 4046, 98^e Congrès des É.-U., M. Fuqua de Floride.
- (24) HR 4047, 98^e Congrès des É.-U., M. Fuqua de Floride.
- (25) HR 4048, 98^e Congrès des É.-U., M. Fuqua de Floride.
- (26) HR 1092, 98^e Congrès des É.-U., M. Nelson de Floride.
- (27) HR 4259, 98^e Congrès des É.-U., M. Mica de Floride.
- (28) HR 4384, 98^e Congrès des É.-U., M. Mica de Floride.

Annexe A

Liste des projets de lois actuels
se rapportant à l'informatique

Canada

Fraude informatique

Projet de loi C-19 (M. MacGuigan)

États-Unis

Fraude informatique

HR 1092 (Nelson, D-Fla)
HR 3075 (Wydan, D-Ore)
HR 4259 (Mica, D-Fla)
HR 4301 (Coughlin, R-Pa)
HR 4384 (Mica, D-Fla)
S 1733 (Trible, R-Va)
S 1920 (Tsongas, D-Mass)
S 2270 (Cohen, R-Maine)

Connaissances en informatique/ordinateurs dans les écoles

HR 91 (Donnelly, D-Mass)
HR 659 (Perkins, D-Ky)
HR 701 (Stark, D-Cal)
HR 2417 (Wright, D-Tex)
HR 2531 (Gingrich, R-Ca)
HR 3750 (Wirth, D-Col)
S 1093 (Dodd, D-Conn)
S 1194 (Danforth, R-Mo)
S 1195 (Bantson, D-Tex)
S 1285 (Hatch, R-Utah)
S 1849 (Lautenberg, D-NJ)

Formation en informatique/études supérieures

HR 1310 (Perkins, D-Ky)
HR 1699 (Perkins, D-Ky)
HR 2483 (LaFalca, K-NY)
HR 3095 (Shannon, D-Mass)
HR 3098 (Stark, D-Cal)
HR 3280 (Cunderson, R-Wisc)
HR 4244 (Jenkins, D-Ca)
HR 4475 (Shannon, D-Mass)
S 530 (Pell, D-RI)
S 874 (Kennedy, D-Mass)
S 1055 (Quayle, R-Ind)
S 1087 (Hatch, R-Utah)
S 1869 (Dodd, D-Conn)
S 2165 (Danforth, R-Mo)

National Computer Institute

S 2204 (Haflin, D-Ala)

National Educational Software Corporation

HR 4228 (Skelton, D-Mo)
HR 4628 (Gore, D-Tenn)

Équipement de machines de bureau

HR 1159 (Alexander, D-Ark)
S 286 (Exon, D-Neb)

Recherche et développement en robotique

HR 1036 (Hawkins, D-Cal)
HR 3485 (Hawkins, D-Cal)
HR 4046 (Fuqua, D-Fla)
HR 4047 (Fuqua, D-Fla)
HR 4048 (Fuqua, D-Fla)

Suppression des droits sur les pièces d'ordinateurs

HR 1410 (St. Germain, D-RI)

Reproduction non-autorisée de microplaquettes et de disques

HR 1028 (Edwards, D-Cal)
S 1201 (Mathias, R-Md)

Grande-Bretagne

Privacy of Information

Data Protection Bill

DOCUMENT: 870-123/007

INTERPROVINCIAL CONFERENCE ON PRIVACY:
INITIATIVES FOR 1984 (SYMPOSIUM)

Transborder Data Flow (TBDF) &
The Continental Communication Pact (CCP):
The Rationale for a Communication Pact

Thomas L. McPhail, Ph.D.
Director and Professor
Graduate Programme in Communications Studies
The University of Calgary



Toronto, Ontario
May 23-24, 1984

Conference on Privacy: Initiatives for 1984

TRANSBORDER DATA FLOW (TBDF) & THE CONTINENTAL COMMUNICATION PACT (CCP):
The Rationale for a Communication Pact

A paper prepared for: "Transborder Data Flow: Toward a Resolution
for the Future: The Trends, the Issues"

Toronto, Canada

May 22-24, 1984

Thomas L. McPhail, Ph.D.
Director & Professor
Graduate Programme in Communications Studies
The University of Calgary
Calgary, Alberta

Transborder Data Flow & the Continental Communication Pact

This paper deals with the issue of transborder data flow (TBDF) ¹ with an eye toward the future. Essentially the paper reviews the major concerns with TBDF including the three most salient items, privacy, employment and sovereignty. The paper then continues to elaborate on three potential scenarios in terms of future trends and concludes with a detailed discussion of the third scenario, the Continental Communication Pact (CCP). The CCP is a proposal for a bilateral sectoral informatics pact with the U.S. that will both maximize the benefits to Canada as an information based economy as well as recognize the natural communication interconnection with the U.S. marketplace.

Introduction:

In the late 1960's and early '70's, the issue of privacy and computers was considered a "hot topic". In fact, as part of the Canadian Telecommission Studies there were a series of privacy related papers that were produced jointly by the Federal Department of Communications and the Federal Department of Justice; yet, little legislative action resulted, but at least the studies indicated an early willingness to examine the issue of privacy in a systematic fashion. This is also true of the issue in terms of other countries', mostly European, initial concerns of privacy and computers. In turn, during the 1970's ^{many} ~~much~~ of the non-economic concerns about computers ^{were} ~~were~~ viewed through the prism of privacy.

But, in the mid 1970's, the debate shifted from privacy to freedom of information issues and access laws resulting from legislative action in various Western nations, particularly the U.S. Now once again, the issue has shifted from these areas to a more broadly based concern about "informatics". Informatics is the marriage of computers and telecommunications in such a way as to produce a blurring of traditional processes and procedures with regards to the storage and access to a multitude of data bases, particularly those controlled by transnational corporations (TNC's).

The means of affecting TBDF may be a consequence of either legislative action, such as Brazil (to be detailed later), or non-legislative action, such as economic barriers, that have the net effect of altering the flow of computerized information and access to computerized data bases. Further examples of non-legislative actions include tariffs, discriminating pricing, idiosyncratic technical standards, import quotas or government subsidies.

Of interest to this Conference is the fact that privacy is now re-emerging as a major issue, not based on traditional concepts, but rather, based upon two new concerns. In this respect privacy has been "born-again" in the TBDF debate.

The first is the introduction of a large scale of private carriers that are now holding individually identifiable information, firms that are referred to as "value added" or "carriers carrier". These satellite services, either through potential competitors to Telesat, COMSAT or

Intelsat, or through I.B.M.'s SBS, are collectively representing a quantum increase in the movement toward essentially non-regulated, or minimally regulated, private TNC communication carriers.

The second development is the continuing increase, estimated 20% a year, of on-line data bases available from a diverse range of information providers and processors, including governments, businesses, and research institutes. Not only are these data bases increasing in actual numbers, but also the ability to move the data electronically between systems in diverse nation states is increasing in parallel. Although I will not deal with it here, clearly the examination of these issues by the Commission of the European Communities, plus the OECD, provide ample evidence of the European communities' concerns with the informatics and privacy.²

It is significant to note that European states place greater importance on privacy and national sovereignty along with other social-cultural and non-economic concerns. Solely economic ^{on} and technical considerations are lower on the agenda for these nation states. To a considerable extent, the Canadian situation and public policy approach to informatics is closer to the European view rather than the U.S. view.

One could argue that in terms of the United States that national sovereignty has not been a major concern for them since they control most of the major actors in the informatics fields. Indeed their sovereignty is being enhanced by the computer revolution. Also to blindly pursue the U.S.'s deregulation strategies in the area of informatics is

not in the public interest from a Canadian perspective.³ I will come back to this later.

The concept of non-economic concerns involving TBDF is reflected in the issue of protection of privacy; particularly concerning information about individuals that has been stored in or ^{is} accessible by foreign-based computer systems. Personal files may contain a wide range of information about an individual's financial, economic, educational, welfare, business and insurance status, medical or criminal history, and political and religious beliefs. The increase and ease of TBDF heightens the concern that foreign governments, corporations or persons, may have access to this personal information. Recipients of data may have the information before the ultimate users do. Loss of control over information introduces new complexities regarding data security.

ECONOMICS & EMPLOYMENT

Another related concern of even more importance to Canada is the implications of TBDF on the economy of our country. A major concern is that employment opportunities are being lost, mainly because the commercial data processing is taking place in the U.S. where multi-national computer firms have their head offices. In 1978 a survey of 400 Canadian subsidiaries of U.S. companies estimated that from \$300 to \$350 million of computing services were imported from U.S. parent companies, and this amount was forecast to increase to \$1.5 billion by 1985.

It is difficult to make accurate predictions on the composition of future employment as pertinent factors which should be examined are subject to economic vagaries on a world scale (i.e. economic growth, political unrest, labour force demographics, foreign trade movements, technological breakthroughs, or decisions of TNC's).

Real employment growth refers only to new jobs added -- not job openings. The projected job expansion has led to the common false assumption that aggregate job growth will be biased toward high technology occupations. Creation of most jobs between 1983 - 1990 will lie in service related sectors with few being related to high technology sectors. Economic growth will favour middle and low level occupations with clerical and service occupations accounting for up to 40% of the employment growth.

Workers in many professions will constantly find their jobs altered by sophisticated computer technologies. Examples of this phenomenon are the increasing utilization of word processors by secretaries, bookkeepers use of computerized financial spread-sheets, the growing implementation of computerized record systems by purchasing and inventory clerks, mechanics use of diagnostic mini-computers and computerized directories employed by telephone operators.

Much automated equipment is currently paced and controlled according to centralized decisions made by managers located in the office, away from the production site. This also allows TNC's to extend and centralize their decision making procedures.

But, despite widespread automation, aggregate skill requirements have changed very little over the last two decades. Automation tends to require less operator skill after certain levels of mechanization are achieved, thus reducing skill requirements. This deskilling phenomenon is evident in the computer technology industry itself. Early computers were large and expensive, manned by programmers and operators with complex skills. As the technology evolved, the tasks and skills involved also changed. Analysts performed the more creative, skilled tasks while programmers and coders were assigned to more tedious and routine functions. Programming became easier with the advancement of user - friendly, menu prompted packages. The new generation of office computers are designed so that knowledge of computer languages or special computer skills are no longer essential.

Office computers currently perform tasks formerly executed by secretaries, emphasizing the reduction of requisite skills needed to perform this type of office work. Word processors correct typing errors and spelling mistakes. As more advanced software is developed highly trained, skilled workers will be in less demand.

A Stanford study by Levine & Rumberger in February, 1983 states:

In addition to this "deskilling" effect it is impossible "that entire classes of skilled workers will disappear or be severely reduced in numbers as their jobs are replaced by robots or computer software." For example, the draftsman could easily be replaced in the not-too-distant future by widespread use of computer-aided design (CAD).

Given that most new jobs will not require higher skill levels and the probable deskilling of many existing occupations, the authors identified three appropriate education policies for the future.

The Stanford study continues:

First, the general educational requirements for creating good citizens and productive workers are not likely to be altered significantly by high technology. Everyone should acquire strong analytic, expressive, communicative and computational skills as well as extensive knowledge of political, economic, social and cultural institutions.

Second, since it is not possible to predict the types of jobs available and selected, and the changes in jobs over a forty-year working life, general academic and vocational preparation should be stressed over specific training. Until the turn of the century, three of the five fastest growing occupations will be: data processing machine mechanics, computer systems analysts, and computer operators and they deal with high-technology products. Employment in these five occupations is projected to increase by over 100 per cent, more than four times the overall employment growth rate.

However, slower growing occupations with a large employment base are expected to contribute far more jobs to the economy than high-technology occupations. In fact, the five occupations expected to produce the most new jobs are all in low-skilled areas: janitors, nurses' aides, sales clerks, cashiers and waiters/waitresses. For example, while 200,000 new jobs for computer systems analysts will be produced in the U.S. between 1978 and 1990, over 600,000 new jobs will be created for janitors. Although

employment in high-tech occupations will increase quickly in percentage terms, the contribution of these jobs to total employment growth will be small.

To put it bluntly, Canada has a vested interest in obtaining its reasonable share of computer related jobs, particularly in data processing, otherwise, as the Stanford Study indicates, we could, as a nation, wind up with a far greater and disproportionate share of the low-skilled variety of jobs.

SOVEREIGNTY

Canada has been investigating domestic communication issues for years. Yet the numerous reports and studies of public policy in all areas of communications have incited a minimum amount of action or sustained attention within the highest levels of our federal government.

One early report, Instant World: A Report on Telecommunications in Canada (1971) was compiled by a study group called "Telecommission." With the cooperation of government, industry, and university personnel, Honorable Eric Kierans, the first Canadian Federal Minister of Communications in 1969 organized a broad ranging study to examine the present and future issues in telecommunications, and to address accompanying social changes. A major observation from the study was that some Canadian information was being stored exclusively in U.S. data banks. At that time, the Canadian insurance industry relied on computerized information from Hartford, Conn. Canadian hardware-makers used a Columbus, Ohio data bank for prices and stock quotes,

and real estate information for four major Canadian cities was held in a Detroit data bank.

In addition to this early deleterious examples of TBDF, the report noted that a continental system existed covering services between the U.S. and Canada. For example, telephone rates were established by the TCTS, (TransCanada Telephone System), the six member companies which shared the U.S. border, and AT & T (American Telephone and Telegraph). However, because regulatory bodies such as the CTC (Canadian Transport Commission), the Department of Communication and the COTC (Canadian Overseas Telecommunications Corporation), were not coordinated in agreements, ad hoc policies developed.

Instant World (1971:96) also addressed the issue of cultural privacy:

This holds that cultures which may be intrinsically rich and satisfying but which are relatively weak in contemporary terms, can neither assimilate inexpensive foreign-produced media content, nor afford to produce material of equally commanding audience impact on their own.

The study recommended that Canada undertake extended R & D efforts to meet Canada's specific media needs. Other recommendations included: the development of multi-disciplinary executives in the industry for effective futuristic planning, as well as multi-lateral discussions involving governments, industry, and universities.

At the management level, the Telecommission advised the expansion of facilities to accommodate Canada's regional diversity, the integration of networks, and particularly, the development of coast to coast digital

transmission systems with linked data bank and information processing organizations.

The main thrust of Instant World (1971:169) is:

To redress the balance, authorities - federal, provincial and municipal alike - may find it worthwhile to collaborate in addressing themselves to these problems so that the greatest possible benefits can be derived from the individual regional, provincial and national opportunities that Canadian computer/communications systems may be expected to provide with a significant impact on social cultural, political and economic activity.

Eight years after the Telecommission study, the Consultative Committee on the Implications of Telecommunications for Canadian Sovereignty (1979), under the direction of Chairman, J.V. Clyne, submitted another report. The Clyne report asserted that Canada should work at being a leader in the field of telecommunications and that its position in the field should be a major focus of public policy. With the concern that Canadian sovereignty was being jeopardized in two fields, the Clyne report (1975:5) stated,

First, Canadians are already being swamped with foreign broadcast programming and a new approach to the problem is urgently required; at the same time, there is a danger that foreign interests may achieve a predominant share of the market for data processing services, and far too much of the information stored in data banks will be of foreign origin. Second, Canada is heavily dependant on imports in telecommunications technology. In certain sectors, such as satellites and information exchange, Canada is in the forefront of competitive technological developments. The exploitation of these developments requires public support that does not entail a vast expenditure of public funds; this is an industrial sector that can create jobs and be competitive on an international scale.

The recurring theme in the Clyne Report was the urgent task of the Canadian government to step into the telecommunications industry with a strategy designed to both preserve Canadian sovereignty and to capitalize on

opportunities in the communication industry. Issues such as broadcasting content, data flow and Canadian ownership of manufacturing and media facilities prompted the Clyne Report to recommend greater government involvement in R & D and in coordinating government and industry efforts.

In The Information Revolution and Its Implications for Canada, (1981), the complexity of communication issues was documented. Because of the fragmented nature of the Canadian economy with its foreign subsidiaries and domestically controlled firms, Canada was described as being vulnerable to conflicting interests -- regional U.S. national, domestic, U.S. foreign. Jurisdictional disputes were documented among the various levels of government, the public lacks awareness of the developing communication issues, and the small Canadian market which cannot provide a strong base for Canada's high technology and electronics industries were outlined. The author adopted the stance that the information society holds both promise and peril for Canadian society, and that government has a key role in maximizing the promise.

More recently the Science Council of Canada reiterated the issues and many of the same recommendations of these previous studies in its Report #33, Planning Now For an Information Society: Tomorrow is Too Late (1982:28). In describing the Canadian electronics industry, the report drew attention to the fact that Mitel and Northern Telecom products can compete on an international level, yet Northern Telecom is only a medium-sized company. Because of the vast amounts of government support in other countries, competition in electronics is as much between countries as companies;

further, 72 of the 100 largest Canadian companies are foreign owned or controlled.

The report stated that a significant component in Canada's future should be a broadly-based chip manufacturing capability for R & D, and effective technology transfer to occur. Since Canada depends heavily on natural resources, the Science Council also recommended improved R & D into technical applications for improved productivity, particularly in the oil and mining industries where extraction is costly. The report attributed Canada's lagging manufacturing sector to the fact that its domestic market of less than 22 million people has not promoted the growth of plants for world scale production and competition.

The Science Council recommended government support of R & D for such things as robotics and specialized computers, but in a reiteration of the rudimentary concern of the previous reports and with renewed urgency, the report (1982:53) stressed:

The creation of a national telecommunications system to provide the infrastructure for the future cultural and economic development of Canada means that telecommunications policy development will require serious attention by the relevant provincial and federal government agencies.

Relative to a future Canadian communication policy, the report (1982:53) continues,

If we do not develop a comprehensive telecommunications policy soon, the resulting confusion will lead to wasted resources, and loss of time in the world race to develop networks and possibly allow the entry into Canada of powerful competing networks from abroad. It is imperative that a policy be enacted designating areas of activity for existing participants, yet providing the

needed flexibility to accommodate new competition and the emergence of new technologies.

Both historically and recently sovereignty and other non-economic concerns have been high on the government agenda with reference to the emerging Information Age.

Whatever implications TBDF may have on Canada, the U.S. has recently indicated a willingness to discuss initiatives on sectoral free trade; among the sectors under consideration is informatics. With both countries committed to the multilateral GATT trading system, bilateral agreements will require special handling. The U.S. has called for cooperation in expanding trade and investment, for the removal of such irritants as the America/Buy Canada provisions, for reducing uncertainties about access, and for removal of other non-tariff barriers. Yet recent U.S. government hearing regarding the steel industry call into question the de facto call for "free trade". U.S. government quotas on Japan auto imports is another example of not so "free trade" approaches when the U.S. perceives itself (or its voters) to be adversely affected.

Essentially pursuing the status quo with regard to TBDF, or even a modified status quo, will continue to see ad hoc policies and policy by incrementalism ultimately resulting in the U.S. being in a favorable or priority position. This is for two major reasons. The first being simply the size, and quickness with which the U.S. government responds in its own vested interests; second, many of the institutions and industries affected by any negotiations are either highly interconnected within the U.S. market or, in fact, are corporately controlled by American parent firms. Therefore the net result of any continuation of simply relying upon a sectoral

approach that responds merely to irritants or to points of conflict will simply see a gradual decline in the Canadian position in the long run. This is true in the three major areas discussed previously, namely, privacy, employment and sovereignty.

OPTIONS:

What then, are the options? If the status quo or a modified status quo and incrementalism are not in the national interest, what other actions may be taken? Well, we may look to the example of Brazil. It is a negative model yet it deserves examination to determine if their model or approach may be applicable to the Canadian situation. Once I have described in some detail the Brazil response to the issues of informatics, privacy, computers and TBDF, I will then spell out a new Canadian option.

In Brazil, the government believes that it does not want to become a "computer colony" ⁴ and this has had led, over the last decade, to a complex network of regulations administered by the Special Informatics Secretariat. Brazil sees independence in computer technology as a matter of sovereignty and national pride, plus the government has taken strong steps to insure the development of a broadly based domestic informatics industry. Nationalism was in fact present at the birth of Brazil's computer industry when, in the mid 1970's, the country's Naval Ministry demanded the security for its computer systems installed in its frigates and destroyers. As a result, the entire issue was taken up by the military government's National Security Council. In 1977 it sponsored the creation of a state computer company,

Cobra, and two years later formed the Special Informatic Secretariat, headed mainly by army and navy engineers.

Since then, an alliance of military officers, local entrepreneurs, and leftist cultural nationalists has formed a coalition around the ideal of protecting and enlarging the emerging Brazilian computer industry. Foreign-owned subsidiaries, principally I.B.M., ⁵ have decreased their total share of the market. In five years their share has fallen from 77 per cent to 53 per cent. Since 1979, domestic sales of Brazilian-made computers has gone from 200 million to almost 700 million. Sales of imported computers have decreased from a high of almost 300 million in 1981, to less than 100 million in 1983.

Brazil's Congress is now debating a law to govern informatics policy, plus the government wants to eliminate the confusion caused by the plethora of ad hoc regulations. No matter what the ultimate decision of Brazil's government will be, the figures indicate that blocking imports has helped the local industry thrive. The government's strong steps have insured the development of a domestic informatics industry. The net losers are the foreign TNC's.

There has been other activity as well.

Among the actions that have been taken internationally are OECD's "Guidelines Governing the Protection of Privacy and the Transborder Flow of Personal Data" (Sept. 1980). The Council of Europe adopted a "Convention for the Privacy of Individuals with Regard to Automatic Processing of Personal Data." In the case of non-personal TBDF, according to the center on Transnational Corporation, about 60 countries have issued some official statement.

TABLE 1

COUNTRY		AUSTRALIA	AUSTRIA	BELGIUM	CANADA	DENMARK	FINLAND	FRANCE	HUNGARY	ICELAND	ISRAEL	JAPAN	LUXEMBOURG	NETHERLANDS	NEW ZEALAND	NORWAY	PORTUGAL	SPAIN	SWEDEN	SWITZERLAND	UNITED KINGDOM	UNITED STATES	WEST GERMANY	EEC	COM	OECD	IDI
TYPE OF REGULATION	LP	L	LP	L	L	LP	L	LP	L	L	P	L	LP	L	L	LP	LP	L	LP	P	L	L		P	P	G	P
PROTECTED PERSONS - Natural Persons		X	X	X	X	X	X	X			X		X	X	X	X		X	X		X	X	X		X	X	
Citizens/Residents Only					X								X		X	X					X						
Legal Persons			X	X		X						X		X	X										X		
NAME-LINKED DATA --EDP/ADP		X	X	X	X	X	X	X			X		X	X	X	X		X	X		X	X	X			X	
Manual Data Processing		X	X		X	X		X					X		X		X				X	X				X	
Collection/Flows/Storage		X	X				X				X		X		X				X						X	X	X
CONTROL - Data Control Boards			X	X	X	X		X				X	X		X		X	X		X		X					
Registration/Licensing			X	X	X		X				X	X			X				X		X	X					
RIGHT TO ACCESS/CHALLENGE		X	X	X	X	X		X			X	X		X	X				X		X	X			X		
Freedom of Information		X	X		X	X	X	X				X	X		X				X		X	X					
LEVEL OF GOVERNMENT - Local		X			X													X		X		X	X				
National		X	X	X	X	X		X		X	X	X	X	X	X	X	X	X			X	X					
International						X						X	X		X		X	X	X					X	X	X	X
REGULATED SECTOR - Public			X	X	X	X		X					X		X				X		X	X					
Private			X	X		X		X				X			X				X					X	X		
Self-regulation							X														X						
ENFORCEMENT Fine								X					X								X						
Victim Compensation														X	X												
Data Confiscated/Destroyed			X									X							X								

KEY

LP = Legislation

L = Legislation

P = Report

G = Guidelines

EEC = European Community

COM = Council of

OECD = Organisation for Economic Co-operation and Development

IDI = Interpower Bureau for Informatics

Note: The countries studied differ in degree of "regulatedness" or in strength of laws and diligence of enforcement. An "X" simply denotes the existence of a condition, not its strength.

Source: Transnational Data Report, 1978-1983, Vols. 1-6; EEC, COE, IBI Reports, OECD Guidelines, and personal correspondence.

Table 1: Transborder data flow, data protection, and privacy regulation in 22 nations

Another example is Sweden which has operated its Data Inspection Board since 1974. Data banks containing information about the activities of individual citizens may not be constructed without permission of the "Inspectorate". If any personal information is intended for use outside Sweden, its issuance depends on special permission.

The trend towards increased data regulation, particularly in Europe, will both ultimately and indirectly affect TBDF in other countries.

A Continental Communication Pact (CCP):

Reports, studies, and commissions attempting to address the TBDF issues have failed to come up with clear-cut Canadian strategies. Questions of privacy, competition, technical change, and regulation on a multi-lateral bases add to the complexity of policy making. In order to deal effectively with the TBDF problem, and in order to be more realistic, the issues should be broken down into something more manageable; such as a single bilateral TBDF agreement with Canada's-largest trading partner - the U.S.

Key assumptions are fundamental to the approach of policy making on the TBDF question. Canada's conviction is that enormous benefits can come with the increases in TBDF. It has been suggested that in order to capitalize on the opportunities in the industry, telecommunications policies should be developed so that Canada can gain entry into the powerful competing networks in the U.S. Interruptions in flows of data between our borders could have negative implications to the computer service industry and almost all industrial activity in Canada. If trade in data, information, and

associated services is to proceed smoothly, Canada must resist temptations to become protectionist. We do not want to become Brazil North.

In establishing a "Continental Communication Pact" (CCP) with the United States, Canada and the U.S. would do well to examine the Auto Pact Agreement of 1965. That agreement was signed to provide duty-free trade by manufacturers in automobiles and parts between the U.S. and Canada. At the time of the Pact, Canada's position in the automobile industry was weak; it was incapable of competing in an international market because of the expense to duplicate U.S. cars in Canadian subsidiaries. The Auto Pact promised to redress the deficit in the sectoral balance of trade and expand production in Canada.⁶

Recently in discussing U.S./Canada economic relations, U.S. Deputy Assistant Secretary of State, James Medas stressed that the Reagan administration is firmly committed to the promotion of freer trade. Last month, Canada and the U.S. signed a safeguard understanding to help assure prompt consultation and cooperation on shared trade concerns. The stage is now being set for a CCP to be established. The U.S. Government has stated a variety of sectors under consideration to the recent Canadian initiative on sectoral free trade, informatics being one of them.

Let us examine the CCP in more detail.

First, the CCP will involve broadcast, telecommunication and computer services/supplies.

Second, it will involve a continental communication grid involving the national governments of the United States and Canada.

Third, communication stakeholders (both public & private, including provincial governments) should be consulted prior to the formation of a CCP.

Just who are the stakeholders. A sample list follows:

- . Computer firms
- . Telesat Canada
- . TCTS & CNCP
- . Provincial telephone companies
- . Cable companies
- . Canadian independent film producers/Telefilm
- . National magazines
- . Hardware suppliers and manufacturers, e.g. Mitel, Northern Telecom, NABU, etc.
- . Software suppliers - information providers, e.g. Infoglobe,
- . Pay TV distributors
- . Advertisers
- . Financial community
- . Investors
- . Governments - relevant federal and provincial departments
- . Labor unions

A few words of explanation. Today we have a series of ad hoc and disjointed, short-run and frequently conflicting policies. In addition, the

federal government's involvement frequently fails to take into account either the provincial role or perspectives.

Meanwhile, DBS, cable, videotex, mobile radio and TBDF are growing on a continental scale precipitating interrelated policy concerns. The CCP would broaden the market for Canadian products, both hardware and software, so as not to be swamped by foreign, mostly American products. To have the CBC and CTV carried on all U.S. cable systems, or new pay service(s) carried on U.S. satellites would financially aid the Canadian services and redress the current imbalance. In addition, it would provide guidelines for Canadian cable companies such as Rogers, Maclean-Hunter, Cablecasting, etc., with franchises in the U.S. The U.S. networks are carried on Canadian cable systems and U.S. pay services are being received by a growing number of Canadian-based earth stations (TVRO's); now the major question is why not have a reciprocal agreement to benefit Canadian manufacturers and software merchants.

A major indicator of Canada's need to develop a communication pact is the trade deficit in computer and office equipment. Chevreau (1983:B 5) indicates that, in 1982, Canada's trade deficit passed the \$2 billion level; exports totalled \$890 million while imports of computers totalled \$3 billion. In spite of government efforts to reduce the deficit through sales of Telidon or Office Communications Systems, Evans Research Corp. of Toronto predicts the deficit will grow to \$5 billion by 1986. The trend towards office automation has increased Canada's demand for foreign office electronics equipment. DOC's throwing a few dollars into office automation projects only masks the more serious underlying structural problems.

There is a greater hope for the marketing of Canadian programming in the U.S. albeit the demand is not yet proven. From the CBC Annual Report (1981-1982), it is apparent that a market does exist for Canadian products, particularly those relating to the arts, in addition to the news programs, *As It Happens* and *Sunday Morning*. These have set the precedent for the possibility of a greater Canadian presence in the American communications scene. An information pact would outline the strategy for the promotion of CBC, NFB, CFDC or Telefilm productions on American networks and theatre screens.

With regards to satellite technology, Canada is being forced into a pact with the U.S. over the issue of future DBS services. Both Canada and the U.S. are seeking to reserve prime satellite orbital slots for future use. While the FCC is planning to establish a DBS system with up to 13 services, Canada is requesting 6 slots with full frequency bandwidth of 500 mhz reserved for each service. Canada's request raises the problem of maximum spacing between each satellite which will be necessary to accommodate the proposed Canadian services, -yet it will also mean that the U.S. will be left with only 4, mainly unfavorable slots. Negotiations will require adjustments to the requests of both countries, although the U.S. favors a system where applications are granted on expression of demand and first-come first-served.

Yet once again, Canada is demonstrating concern for the preservation of its sovereignty by seeking an orbital slot for each of its five time zones and an additional slot for French programming for Quebec. While Canada does not have the economic resources to develop these services immediately, it is

seeking to prevent the U.S. from absorbing all the available slots now. (It is to be remembered that other smaller countries, particularly in South America, are hoping to use DBS services in the future, and are looking at the same parking spaces that Canada and U.S. are hoping to capture.)

Another example of the informal movement toward a CCP is a recent agreement between DOC & NASA to establish a cooperative effort to define a single space programme to meet mobile communication needs in both countries. This joint effort may result in a common mobile satellite system offering similar services in both countries.

The issues of both content and hardware/software sovereignty could be addressed by the negotiation of a joint satellite serving both the American and Canadian public. Canadian strategy on this point would involve a bilateral agreement with the United States regarding the division of revenues from the joint satellite network; the equity of content/carrier status, and the equal division of American and Canadian programming services provided by the satellite, plus shared R & D. The R & D aspect will protect Canada from becoming a technological serf in the Information Age.

A final point. This CCP proposal is aimed at strengthening Canadian cultural industries; the status-quo requires writers, producers, directors, etc. to continually water-down Canadian references, history, themes, etc. to accommodate U.S. commercial concerns. With the CCP the carriage would be guaranteed and therefore a Canadian perspective dealing with Canadian ideas, norms, perspectives, etc. (like the Australian film industry) will be possible. The CCP is not aimed at a mass audience philosophy but rather is

consistent with the narrow casting or tiering approach of evolving North American cable-satellite hybrid systems.

Without such a bold enterprising move as the CCP, Canada will lose its already weak position with regards to hardware technology and software. The status quo is really a closet policy giving Canada the worst of both worlds (hardware and software). Ad hoc policies are not sufficient to guarantee a significant Canadian presence in the international and continental scene, and market forces have historically indicated that American programming has a significant edge over Canadian production prospects. Therefore, the urgency to develop a CCP with the United States is increasing and it is up to Canadian policy-makers to explore the opportunities in order to secure Canadian privacy, sovereignty, and employment opportunities in the Information Age.

CONCLUSIONS

In sum, this paper has reviewed the area of TBDF through the prism of privacy, in part, with additional concern for the areas of employment and national sovereignty. Also discussed were three models of approach for future action in the area of TBDF.

First, an examination of the status quo, or modified status quo, which will see the Canadian position deteriorate over time in favor of both the U.S. government position as well as for the benefit of the commercial and corporate interests of U.S. communication industries was discussed.

Second, an examination of a restrictive TBDF model, particularly in Brazil, was examined as well as outlining their rationale and actions in terms of the general area of informatics.

Third, a new plan was outlined and elaborated upon dealing with a Continental Communication Pact (CCP). The CCP was outlined in terms of the various stakeholders involving broadcast, telecommunication, and computer firms. In addition, examples were cited to demonstrate the range of issues, a possible procedural approach involving both the public and private sector as well as provincial governments, and finally, comments were made concerning the ability of the CCP to both enhance and enrich the cultural sovereignty of Canada as a nation state, as well as provide for a more equitable distribution of research and development for future communication technologies, plus some enhanced likelihood of additional manufacturing jobs being available in Canada in the high technology area.

ENDNOTES

1. For the purpose of this paper "transborder data flow may be defined as the transmission of machine readable data and information over trans national computer and other electronic communication systems for the purpose of storage, retrieval, or processing." "Transborder Data Flow, Informatics, and National Policies", Journal of Communication, Winter, 1984, p. 154.
2. The OECD data declaration will be discussed in Paris on July 2-3, 1984 by the OECD Working Party on TBDF.
3. It is somewhat ironic that in 1984 the nation with the greatest investment in international communication affairs, the United States, is also the same nation that is doing its utmost to close down those international fora or associations that are most likely to aid it in its goals, whatever they be, whether it is free flow of information, TBDF, or free trade, or rational and efficient use of the international spectrum space. Consider the following that points the accusing finger at the Reagan administration for manipulating U.S. policy and participation in international communication affairs in a deleterious, disruptive and negative fashion.

"U.S. Off Course

On the contrary, the U.S. is moving in the reverse direction, abandoning or neutralizing a forum capable of accommodating a broad, varied membership and of accepting revised agendas and new perspectives. The U.S. proposes to leave the United Nations Educational, Scientific and Cultural Organization (UNESCO), partly because of its attention to disputed international communication practices and conditions. The U.S. is pressing the International Telecommunication Union no less (ITU) to confine itself to technical concerns. It is reducing its participation in the U.N. Committee on Information and in the legal and technical sub-committees looking at future spaces communications for the Committee on the Peaceful Uses of Outer Space. It stands apart from the Intergovernmental Bureau on Informatics (IBI) and the U.N. Center for Transnational Corporations, both of which exhibit deep interest in transborder data flow problems involving the Third World." Chronicle of International Communication, April, 1984, Volume 5, Number 3, page 7.

4. For detailed discussion see: T.L. McPhail, Electronic Colonialism: The Future of International Broadcasting & Communication, (Beverly Hills, Calif.: Sage Publications, 1981). Also refer to other writings by the same author listed in the bibliography.
5. I.B.M. also has some domestic (U.S.) critics.

"Moreover, given I.B.M.'s recently demonstrated litigiousness with its smallest opponents, would be competitors have experienced a deep chill, especially if there are former I.B.M. employees. The danger is that a class of 'technological serfs' is being created -- those who once worked for I.B.M. are now forever subject to trade secret litigation. It is a disturbing paradox that, now freed from (U.S.) government litigation, I.B.M. is using litigation to stifle competition and block the diffusion of technology in elevation, especially in the main frame plug-compatible markets." New York Times, Sunday, May 13, 1984, page 2F.

6. I will not discuss the details or results of the auto-pact here, but Beigie (1970) and others have studied it elsewhere.

References:

- Beigie, Carle E. "The Canada-U.S. Automotive Agreement: An Evaluation." Canadian American Committee, Canada. 1970.
- "Brazil's Prickly Computer Policy". The New York Times, April 29, 1984. p. 12F.
- Chevreau, Jonathan, "Computer, Office Equipment Showing Higher Trade Deficit." Globe and Mail, February 11:85, 1983.
- Clyne, J.V. "Telecommunications and Canada, Consultative Committee on the Implications of Telecommunications for Canadian Sovereignty." Minister of Supply and Services, Canada. 1979.
- "Council of Europe Convention for the Protection of Individuals with Regard to Automated Processing of Personal Data." Transnational Data Report 3(6), 1980.
- Crawford, Morris H. "The IBI Transborder Data Flow Conference: An American View." Transnational Data Report 3(3-4), 1980, pp. 38-41.
- Cundiff, W.E. and Mado Reid, "Issues in Canadian/U.S. Transborder Computer Data Flows." Institute for Research on Public Policy, Toronto: Butterworth & Co. Canada, Ltd. 1979.
- European Communities, Commission. "European Society Faced with the Challenge of New Information Technologies: A Community Response." Brussels: European Economic Community, 1979.
- "Europe/North America: A One-Way Flow." Information Systems 30, 1979.
- Ganley, Oswald G., "The United States-Canadian Communications and Information Resources Relationship and Its Possible Significance for Worldwide Diplomacy." Program on Information Resources Policy, Working Paper, Cambridge, Mass.: Harvard University. 1979.
- Hamelink, Cees J. "Informatics: Third World Call for New Order." Journal of Communication 29(3), Summer 1979, pp. 144-148.
- The Impact of Transnational Data Flows on Developing Countries. J.C. Grant. An address to the Conference on Information, Economics, and Power North South Dimension. The University of Western Ontario, School of Journalism. March 10, 1984.
- Instant World, "A Report on Telecommunications in Canada", Ottawa: Information Canada. 1971.
- Issues in Canadian/U.S. Transborder Computer Data Flows. W.E. Cundiff and Mado Reid (Eds.) Proceedings of a conference sponsored by the Institute for Research on Public Policy. 1978.
- Lesser, Barry, "The Implications of the Federal and Provincial Proposals for Regulating Telecommunications: An Economist's Perspective, in

- Telecommunications Regulation and the Constitution.", Robert Buchan, Christopher Johnston (Eds.). Montreal: The Institute for Research on Public Policy. 1982.
- Lester, R.M., "Communications and Transborder Information Flows." The Conference Board of Canada Business Outlook Conference, unpublished paper. 1981.
- Levine, H., & Rumberger, R., Stanford University, Project Report No. 83-A 4.
- McPhail, Thomas L., "The Future of Canadian Broadcasting: Proposed Revision of Regulatory Mechanisms and Policies", in The Crisis in Canadian Broadcasting. (Ottawa: Canadian Broadcasting League, 1976).
- McPhail, Thomas L., Electronic Colonialism: The Future of International Broadcasting and Communication. (Beverly Hills, Calif.: Sage Publications, 1981), pp. 259.
- McPhail, Thomas L., "Telematics, Telejournalism in Public Policy Concerns", Competition in the Information Economy, Horizon House, 1981, pp. 417-420.
- McPhail, Thomas L., "The Future of Canadian Communications", Communications in Canadian Society, B. Singer, (ed.) Toronto: Addison-Wesley 1983, pp. 73-82.
- McPhail, Thomas L., "Direct Broadcast Satellites: The Demise of Public and Commercial Policy Objectives", Telecommunications in the year 2000: National and International Perspectives, (with S. Judge), Indu Singh, (ed.) (Ablex Publishing Corporation, Norwood, New Jersey, 1983), pp. 72-79.
- Medas Points Directions in U.S./Canada Economic Relations. James Medas, U.S. Deputy Assistant Secretary of State. Text of Speech delivered in Montreal to Canadian Club of Montreal, The Chambre de Commerce du District de Montreal, and the Montreal Board of Trade. March 19, 1984.
- Melody, William, "Are Satellites the Pyramids of the 20th Century?" In Search, Volume VI, No. 2 Spring pp. 2-9.
- Organization for Economic Cooperation and Development. Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Paris: OECD, 1981.
- Planning Now for an Information Society - Tomorrow is Too Late. Science Council of Canada - Committee on Computers and Communication. 1982.
- Read, William H. "Foreign Policy: The High and Low Politics of Telecommunications." In Anthony G. Oettinger, Paul J. Berman, and William H. Read (Eds.) High and Low Politics: Information Resources for the '80s. Cambridge, Mass.: Ballinger, 1977.

- Robinson, Peter. "Some Economic Dimensions of TDF." Transnational Data Report 3(3-4), 1980, pp. 18-19.
- Schiller, Herbert I. "Computer Systems: Power From Whom and From What?" Journal of Communication 28(4), Autumn 1978, pp. 184-194.
- Science Council of Canada, "Planning Now for an Information Society: Tomorrow is Too Late." Minister of Supply and Services, Ottawa. 1982.
- Serafini, S. and M. Andrieu, "The Information Revolution and Its Implications for Canada." Communications Economics Branch, Department of Communications, Minister of Supply and Services, Ottawa. 1980.
- Silverman, Paul E. "The Evolving Market for International Communications." Telecommunications, april 1978, pp. 25-30.
- "Survey Shows 35 Countries to Regulate Data Flows." Transnational Data Report 1(7), 1978.
- Telecommunications and Canada. Consultative Committee on the Implications of Telecommunications for Canadian Sovereignty.
- "Trade Barriers to Telecommunications, Data and Information Services." Transnational Data Report 5(4), 1982, pp. 179-185.
- Traded Computer Services: A Bilateral Beginning. An address by Rowland C. Frazee, Chairman and Chief Executive Officer, The Royal Bank of Canada. Delivered at the Bookings Institution Washington, D.C. April 10, 1984.
- Transborder Data Flow a Hot Issue. Lawrence Surtees, Globe and Mail, February 24, 1984.
- Transborder Data Flows: A Multinational Issue. C.J. Maule. An Article appearing in the Foreign Investment Review, Autumn 1982.
- Trubow, George B. "Privacy, Policy and Computers." Paper presented to the Computer Privacy and Security Symposium, "Top Secrets 1981," sponsored by Honeywell Information Systems, Inc., Phoenix, Arizona, April 1981.
- Wigand, Rolf T. "Direct Satellite Broadcasting: Selected Social Implications." In M. Burgoon (Ed.) Communication Yearbook 6. Beverly Hills, Cal.: Sage, 1982, pp. 250-288.
- Wigand, Rolf T., Shipley, C. & Shipley, W., "TBDF, Informatics, & National Policies", Journal of Communication 24(1), Winter 1984, pp. 153-175.
- Williams, J.K. "European Data Protection - A Business Viewpoint." Transnational Data Report 5(3), 1982, pp. 156-157.

DOCUMENT: 870-123/007

CA1
Z4
-252

CONFÉRENCE INTERPROVINCIALE SUR LA PROTECTION DES RENSEIGNEMENTS

PERSONNELS: MESURES POUR 1984 (COLLOQUE)

La transmigration des données (TMD) et
le Pacte continental sur les communications (PCC):
la justification d'un Pacte sur les communications

Thomas L. McPhail, Ph.D.

Directeur et professeur

Programme des études supérieures en communications

Université de Calgary



Toronto, Ontario

23-24 mai 1984

Conférence sur la protection des renseignements personnels

Mesures pour 1984

CONFÉRENCE INTERPROVINCIALE SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS: MESURES POUR 1984 (COLLOQUE)

Document préparé pour:

"La transmigration des données;

Vers une solution de l'avenir;

tendances et problèmes"

Toronto, Canada

22-24 mai 1984

Thomas L. McPhail, Ph.D.

Directeur et professeur

Programme des études supérieures en communications

Université de Calgary

Calgary, Alberta

La transmigration des données et le Pacte continental sur les communications

Dans ce document, nous traiterons du problème de la transmigration des données (TMD)¹ dans une perspective d'avenir. Ce document couvre essentiellement les principaux problèmes suscités par la TMD, et notamment les trois questions les plus importantes: la protection des renseignements personnels, l'emploi et la souveraineté. Le document se poursuit par la description de trois scénarios possibles pour les tendances futures, et se conclut par un examen détaillé de la troisième option, le Pacte continental sur les communications (PCC). Le PCC constitue une proposition de pacte bilatéral sectoriel dans le domaine de l'informatique avec les États-Unis, qui permettrait de maximiser les avantages qu'en retirerait le Canada compte tenu de son économie fondée sur l'information et consacrerait la reconnaissance de son interconnection naturelle avec le marché des États-Unis.

Introduction

Le problème de la protection des renseignements personnels et des ordinateurs était considéré comme un "sujet brûlant" dès la fin des années 60 et le début des années 70. En fait, le ministère fédéral des Communications et le ministère fédéral de la Justice ont publié une série d'études sur la protection des renseignements personnels, dans le cadre des Études de la Télécommission canadienne; ces études n'ont produit que peu de résultats législatifs, mais elles indiquaient à tout le moins que les autorités étaient déjà déterminées à examiner systématiquement le problème

de la protection des renseignements personnels. Les mêmes commentaires pourraient être faits à l'égard d'autres pays, pour la plupart européens, qui se sont préoccupés très tôt du problème de la protection des renseignements personnels et des ordinateurs. Durant les années 70, de nombreuses préoccupations non économiques au sujet des ordinateurs furent également exprimées à travers le prisme de la protection des renseignements personnels.

Toutefois, au milieu des années 70, on délaissa quelque peu les questions de protection des renseignements personnels et le débat s'orienta sur les problèmes relatifs à la liberté d'accès à l'information et aux lois sur l'accès à l'information adoptées dans divers pays occidentaux, et particulièrement aux États-Unis. Une fois de plus, le débat s'est de nouveau déplacé vers une préoccupation plus large à l'égard de "l'informatique". L'informatique résulte du mariage entre les ordinateurs et les communications, ce qui tend à estomper quelque peu la distinction entre les procédés et procédures traditionnelles en ce qui concerne l'emmagasinement d'une multitude de bases de données et l'accès à celles-ci, et particulièrement les bases de données contrôlées par des sociétés multinationales (SM).

Les entraves à la TMD peuvent résulter d'une action législative, comme dans le cas du Brésil (que nous expliquerons ci-dessous), ou d'autres types de mesures, telles les barrières économiques, qui entravent le flux des renseignements informatisés et l'accès aux bases de données informatisées. Parmi les autres exemples de mesures non législatives, on peut notamment relever: les tarifs, les pratiques de prix discriminatoires, les normes

techniques distinctes, les quotas d'importation ou les subventions gouvernementales.

Cette Conférence sera particulièrement sensible au fait que la protection des renseignements personnels redevient maintenant un problème majeur, non pas en raison de concepts traditionnels, mais plutôt en raison de deux préoccupations nouvelles. On peut dire en ce sens que le débat sur la TMD fait "renaître" le problème de la protection des renseignements personnels.

La première de ces préoccupations concerne l'avènement d'importantes sociétés de télécommunication qui détiennent maintenant des renseignements permettant d'identifier les individus, des entreprises que l'on qualifie de "services à valeur ajoutée" ou de "télécommunicateurs au service des télécommunicateurs". Ces services par satellite, qu'ils soient offerts par des concurrents potentiels de Telesat, COMSAT ou Intelsat, ou par le réseau SBS de I.B.M., traduisent une accélération collective du mouvement vers une situation où l'on retrouverait principalement des sociétés multinationales privées de télécommunication non réglementées ou assujetties à une réglementation minimale.

Le deuxième facteur est l'augmentation continue, qu'on évalue à 20% par an, des bases de données en direct auxquelles il est possible d'avoir accès par l'intermédiaire de divers fournisseurs d'information et de sociétés spécialisées dans le traitement de l'information, et notamment les gouvernements, les entreprises et les instituts de recherche. Non seulement le nombre réel de ces bases de données augmente-t-il, mais il

s'accompagne d'une augmentation parallèle des possibilités de transfert électronique des données entre les systèmes de divers états. Bien que je n'en traiterai pas ici, le fait que la Commission des communautés européennes et l'OCDE étudient ces questions illustre bien les préoccupations des communautés européennes à l'égard de l'informatique et de la protection des renseignements personnels.²

La grande importance accordée par les États européens à la protection des renseignements personnels et à la souveraineté nationale ainsi qu'à d'autres préoccupations socio-culturelles et à caractère non économique est révélatrice. Pour ces États, les considérations purement économiques ou techniques n'ont qu'une importance secondaire. La situation canadienne et les grandes orientations en matière d'informatique au Canada se rapprochent plus, pour une large part, du point de vue européen que de celui des États-Unis.

On pourrait soutenir que la souveraineté nationale ne constitue pas une préoccupation majeure pour les États-Unis, puisqu'ils contrôlent la plupart des principaux acteurs dans le domaine de l'informatique. On pourrait même dire que leur souveraineté est raffermie par la révolution des ordinateurs. En outre, du point de vue canadien, il ne serait pas dans l'intérêt public d'adhérer aveuglément à la stratégie de déréglementation des États-Unis dans le domaine de l'informatique.³ Je reviendrai sur ce point plus tard.

Les préoccupations non économiques à l'égard de la TMD se reflètent dans le problème de la protection de la vie privée et en particulier au

sujet des renseignements personnels emmagasinés dans des systèmes informatisés établis à l'étranger ou auxquels on peut avoir accès par ce genre de système. Les dossiers personnels peuvent contenir un large éventail de renseignements au sujet d'un individu: renseignements financiers et économiques; son niveau académique; s'il reçoit des prestations de bien-être social; l'état de ses affaires; les montants d'assurance souscrits, ses antécédents médicaux et criminels; et ses opinions politiques ou ses convictions religieuses. La croissance et la banalisation de la TMD avivent les craintes que des gouvernements étrangers, des sociétés ou des personnes puissent avoir accès à ces renseignements personnels. Les responsables de la conservation des données peuvent obtenir l'information avant même les utilisateurs. La perte de contrôle sur l'information suscite de nouveaux problèmes en ce qui concerne la sécurité des données.

L'ÉCONOMIE ET L'EMPLOI

Les conséquences de la TMD sur l'économie de notre pays constituent un sujet de préoccupation connexe encore plus important pour le Canada. L'une des principales préoccupations concerne la perte d'emplois, principalement en raison du fait que le traitement des données commerciales s'effectue aux États-Unis, où les entreprises multinationales d'informatique ont établi leur siège social. Un sondage mené en 1978 auprès de 400 filiales canadiennes de compagnies des États-Unis estimait à 350 millions de dollars les services d'informatique importés de compagnies-mères établies aux États-Unis, et il était prévu que ce montant passerait à 1,5 milliard de dollars en 1985.

Il est difficile de faire des prédictions exactes sur la composition de la main-d'oeuvre dans l'avenir, puisque les facteurs dont il faut tenir compte dépendent de fluctuations économiques mondiales (c.-à-d. la croissance économique, l'agitation politique, les variations démographiques de la force de travail, les fluctuations du commerce étranger, les innovations technologiques, ou les décisions des sociétés multinationales).

La croissance réelle de l'emploi ne se traduit que par les nouveaux emplois créés, et non par le nombre d'emplois disponibles. Les projections sur la croissance de l'emploi ont entraîné l'hypothèse erronée, mais néanmoins répandue, que la croissance globale de l'emploi sera concentrée dans les occupations du secteur de la haute technologie. Or, la plupart des emplois créés entre 1983 et 1990 le seront dans le secteur des services, et très peu dans celui de la haute technologie. La croissance économique se fera surtout dans les emplois des niveaux intermédiaire et inférieur, les emplois de bureau et de service représentant jusqu'à 40% de la croissance de l'emploi.

La technologie informatique de pointe viendra constamment modifier la physionomie de l'emploi des travailleurs de nombreuses professions. On peut illustrer ce phénomène par plusieurs exemples: les secrétaires utilisent de plus en plus les appareils de traitement de textes; les comptables utilisent de façon croissante les tableaux de ventilation financiers informatisés; et l'utilisation croissante de systèmes d'inventaire informatisés par les commis aux achats et inventaires, de mini-ordinateurs à diagnostic par les mécaniciens, et d'annuaires informatisés par les standardistes.

Une grande partie de l'équipement automatisé est actuellement contrôlé et son fonctionnement planifié en fonction de décisions prises par des gestionnaires installés dans un bureau loin des lieux de production. Cela permet également aux sociétés multinationales d'étendre et de centraliser leurs procédures de prise de décision.

Malgré cette automatisation généralisée, les exigences globales quant aux qualifications ont très peu changé durant les deux dernières décennies. L'automatisation tend à exiger moins de qualifications de la part de l'opérateur, une fois atteint un certain niveau de mécanisation, ce qui réduit la nécessité des qualifications. Ce phénomène de "déspécialisation" se manifeste clairement dans l'industrie de la technologie des ordinateurs elle-même. Les premiers ordinateurs étaient volumineux et coûteux, et étaient utilisés par des programmeurs et des opérateurs possédant des connaissances complexes. La technologie évoluant, les tâches et les qualifications requises ont également évolué. Les analystes ont commencé à s'occuper des tâches plus créatives, nécessitant plus de connaissances tandis que les tâches plus fastidieuses et répétitives ont été confiées aux programmeurs et aux codeurs. La programmation est devenue plus facile avec l'avènement des progiciels conviviaux à guidage par menu. La nouvelle génération des ordinateurs de bureau est conçue de façon à ce qu'il ne soit plus nécessaire de connaître les langages informatiques, ou de posséder des connaissances particulières en ce domaine.

Les ordinateurs de bureau accomplissent maintenant des tâches autrefois exécutées par les secrétaires, soulignant par le fait même la baisse des qualifications nécessaires pour accomplir ce genre de travail de

bureau. Les appareils de traitement de textes corrigent les erreurs de frappe et les fautes d'orthographe. Le perfectionnement des logiciels s'accompagnera d'une baisse de la demande des employés ayant reçu une longue formation spécialisée.

On relève les commentaires suivants dans une étude faite en février 1983 par MM. Levine et Rumberger, de l'Université Stanford:

"Outre cet effet de 'désécialisation' il est possible que 'des catégories entières de travailleurs spécialisés disparaissent, ou que leur nombre soit drastiquement réduit, lorsque leurs tâches seront accomplies par des robots ou par des logiciels d'ordinateur.' Par exemple, les dessinateurs pourraient fort bien être remplacés dans un avenir assez rapproché par l'utilisation généralisée de la conception assistée par ordinateur (CAI)."

Étant donné que la plupart des nouveaux emplois n'exigeront pas de qualifications accrues et qu'un grand nombre des emplois existant deviendront moins spécialisés, les auteurs ont identifié trois orientations qu'il conviendrait de prendre à l'avenir dans le domaine de l'éducation.

L'étude de Stanford poursuit:

"Premièrement, il est peu probable que la haute technologie modifie de façon sensible les connaissances générales requises pour former de bons citoyens et des ouvriers productifs. Tous devront se forger de bonnes aptitudes d'analyse, d'expression, de communication

et de calcul, et acquérir une connaissance approfondie des institutions politiques, économiques, sociales et culturelles."

Deuxièmement, étant donné qu'il est impossible de prédire les genres d'emplois qui seront disponibles et choisis, ni l'évolution du secteur de l'emploi au cours d'une vie professionnelle s'étendant sur 40 ans, on devra mettre l'accent sur la préparation académique et professionnelle générale, plutôt que sur une formation spécifique. Jusqu'au tournant du siècle, trois des cinq occupations qui connaîtront la croissance la plus rapide seront les mécaniciens de machines de traitement de données, les analystes de systèmes d'ordinateur et les opérateurs d'ordinateur; il s'agit dans tous les cas de produits de haute technologie. On a prévu que l'emploi dans ces cinq occupations augmenterait de 100%, soit plus de quatre fois le taux de croissance général de l'emploi.

On s'attend toutefois à ce que les secteurs à croissance moins rapide employant un grand nombre de personnes créent beaucoup plus d'emplois dans l'économie que les occupations reliées à la haute technologie. En fait, il est prévu que la plupart des nouveaux emplois seront créés dans cinq occupations nécessitant peu de qualifications: concierges, aide-infirmières, vendeurs, caissiers et serveurs/serveuses. Par exemple, 200 000 nouveaux emplois d'analyste de systèmes d'ordinateur seront créés aux États-Unis entre 1978 et 1990, mais 600 000 nouveaux emplois de concierge seront créés durant la même période. Bien que le pourcentage de l'emploi dans les occupations reliées à la haute technologie augmentera rapidement, ces types d'emplois contribueront peu à la croissance totale de l'emploi.

Exprimé en termes directs, cela signifie que le Canada a tout intérêt à obtenir une part raisonnable des emplois reliés à l'informatique, et particulièrement dans le domaine du traitement des données sinon, comme l'indique l'étude de Stanford, notre pays pourrait hériter d'une part disproportionnée des types d'emplois peu qualifiés.

LA SOUVERAINETÉ

Le Canada a mené des enquêtes sur les problèmes de la communication au niveau national pendant des années et pourtant, les nombreux rapports et études sur les orientations publiques dans tous les domaines des communications n'ont suscité qu'un minimum de mesures, ou ont peu retenu l'attention des échelons les plus élevés de notre gouvernement fédéral.

L'un des premiers rapports, intitulé Instant World: A Report on Telecommunications in Canada (1971), a été rédigé par un groupe d'étude appelé la "Télécommission". Avec la coopération du gouvernement, de l'industrie et de chercheurs universitaires, l'honorable Eric Kierans, le Premier ministre fédéral des communications au Canada a lancé en 1969 une vaste étude, en vue d'examiner les problèmes actuels et futurs des télécommunications ainsi que les modifications sociales allant de pair. Une observation majeure a été faite dans cette étude: certains renseignements canadiens étaient uniquement emmagasinés dans des banques de données des États-Unis. À l'époque, l'industrie canadienne de l'assurance utilisait des renseignements informatisés en provenance de Hartford, Connecticut; des manufacturiers canadiens de quincaillerie utilisaient une banque de données de Columbus, Ohio, pour leurs prix et leurs inscriptions

en bourse; et les renseignements sur le marché mobilier de quatre grandes villes canadiennes se trouvaient dans une banque de données de Détroit.

Outre ces exemples précoces de TMD préjudiciable, le rapport soulignait l'existence d'un système continental régissant les services entre les États-Unis et le Canada. Par exemple, les taux des communications téléphoniques étaient fixés par le STT (Système de téléphone transcanadien), soit les six compagnies membres de cet organisme qui se partageaient la frontière des États-Unis et AT & T (American Telephone and Telegraph). Toutefois, étant donné que les organismes réglementaires comme la CCT (Commission canadienne des transports), le ministère des Communications et la SCTO (Société canadienne des télécommunications outre-mer) n'avaient pas concerté leurs efforts par le biais d'ententes, les principes directeurs ont été élaborés ponctuellement, en fonction des besoins.

Le problème de l'autonomie culturelle a également été abordée dans Instant World (1971:96):

"Cela signifie que des cultures qui peuvent être intrinsèquement riches et gratifiantes mais qui sont relativement faibles en termes contemporains, ne peuvent assimiler le contenu des émissions produites à bas prix à l'étranger, ni produire elles-mêmes des émissions susceptibles de capter l'intérêt de leur auditoire."

L'étude recommandait que le Canada entreprenne des efforts de recherche et de développement soutenus afin de répondre à ses besoins spécifiques

dans le domaine des médias. Elle contenait d'autres recommandations, notamment sur la formation de directeurs polyvalents en milieu industriel en vue d'une planification efficace à long terme, ainsi que sur la tenue d'échanges multilatéraux entre les gouvernements, l'industrie et les universités.

À l'échelon de la direction, la Télécommission recommandait l'expansion des locaux afin de répondre à la diversité régionale du Canada, l'intégration des réseaux et, surtout, la mise sur pied de systèmes transcanadiens de transmission numérique, reliés à des banques de données et à des organismes de traitement de l'information communs.

Le principal thème de Instant World (1971:169) consiste:

"à redresser l'équilibre; toutes les autorités - fédérale, provinciales et municipales - ont intérêt à s'attaquer ensemble à ces problèmes afin que l'on puisse bénéficier au maximum des avantages que les systèmes canadiens d'informatique et de communication peuvent apporter au plan individuel, régional, provincial et national, ce qui aura des conséquences importantes sur les activités sociales, culturelles, politiques et économiques."

Huit ans après l'étude de la Télécommission, le Comité consultatif des télécommunications et de la souveraineté canadienne (1979) présidée par M. J.V. Clyne, a publié un autre rapport. Celui-ci soutenait que le Canada devrait s'efforcer de devenir un chef de file dans le domaine des télécommunications et que la position du Canada dans ce domaine devrait

être une préoccupation majeure pour les autorités. Craignant que la souveraineté canadienne ne soit mise en danger sur deux fronts, le rapport Clyne (1979:5) déclarait ce qui suit:

"En premier lieu, il faut se rendre à l'évidence que les auditoires canadiens sont submergés par les émissions étrangères et que cette question doit faire l'objet, à partir de critères nouveaux, d'un réexamen immédiat. Dans le même ordre d'idée, il est à craindre que des intérêts étrangers dominent éventuellement le secteur des services informatiques et qu'une proportion beaucoup trop grande des données stockées dans les banques d'information soient d'origine étrangère. En second lieu, le Canada est aujourd'hui dans l'obligation d'importer un grand nombre de produits dont il a besoin en technologie des télécommunications.

Pourtant, nos innovations technologiques dans le domaine de la télécommunication par satellite et la transmission de l'information, par exemple, placent le Canada à la fine pointe du progrès. Leur mise en valeur n'exigerait pas d'importantes mises de fonds gouvernementales, puisqu'il s'agit d'une industrie de main-d'oeuvre qui saurait se défendre sur les marchés internationaux."

Un thème revient constamment dans le rapport Clyne, soit que le gouvernement canadien devait s'impliquer rapidement dans l'industrie des télécommunications, armée d'une stratégie visant à la fois à préserver la souveraineté canadienne et à profiter des occasions offertes dans l'industrie des communications. Des problèmes comme le contenu des

émissions, les échanges de données et la propriété canadienne des entreprises manufacturières et des entreprises oeuvrant dans le domaine des médias, incitèrent les auteurs du rapport Clyne à recommander au gouvernement d'intensifier ses efforts dans la recherche et le développement, et dans la coordination des efforts du gouvernement et de l'industrie.

Le rapport intitulé The Information Revolution and Its Implications for Canada (1981) s'est penché sur le caractère complexe des problèmes de communication. Étant donné la nature fragmentaire de l'économie canadienne, avec ses filiales de sociétés étrangères et ses entreprises contrôlées au pays même, le Canada était perçu comme la cible vulnérable d'intérêts contradictoires: régionaux-nationaux, intérieurs-étrangers. Le rapport faisant également état des conflits de compétence entre les divers paliers de gouvernements, de la méconnaissance du public à l'égard des nouveaux problèmes de communication, et du faible marché canadien qui ne peut constituer une base solide pour les industries canadiennes de la haute technologie et de l'électronique. L'auteur se disait d'avis que la société de l'information était à la fois riche de promesses et de périls pour la société canadienne, et que le gouvernement devait jouer un rôle majeur afin de tirer le plus grand parti possible de ce potentiel.

Plus récemment, le Conseil des sciences du Canada a de nouveau soulevé ces problèmes et a réitéré un grand nombre des recommandations faites dans ces études antérieures, dans son Rapport #33 intitulé Préparons la société informatisée: demain, il sera trop tard (1982:28). Décrivant l'industrie canadienne de l'électronique, le rapport souligne que les produits des

sociétés Mitel et Northern Telecom sont concurrentiels sur le marché international, alors que Northern Telecom n'est qu'une compagnie de taille moyenne. Étant donné les subventions gouvernementales importantes accordées dans d'autres pays, la concurrence dans le domaine de l'électronique se livre autant entre les pays qu'entre les compagnies; en outre, 72 des 100 plus importantes compagnies canadiennes sont sous propriété ou contrôle étrangers.

Le rapport déclarait que l'avenir du Canada en ce domaine dépendait en bonne partie de la mise sur pied d'une importante industrie de fabrication de "puces" adaptées à la recherche et au développement, et des transferts de technologie. Étant donné que le Canada est très dépendant de ses ressources naturelles, le Conseil des sciences recommandait également l'intensification des activités de recherche et de développement dans le domaine des applications techniques permettant d'améliorer la productivité, particulièrement dans les industries du pétrole et des mines où l'extraction est coûteuse. Ce rapport attribuait la faiblesse du secteur manufacturier du Canada à la taille réduite de son marché intérieur (moins de 22 millions de personnes) qui n'a pas encouragé l'expansion des usines en vue d'une production et d'une concurrence à l'échelle mondiale.

Le Conseil des sciences recommandait au gouvernement d'appuyer la recherche et le développement dans des domaines comme la robotique et les ordinateurs spécialisés mais, réitérant les préoccupations exprimées sommairement dans les rapports antérieurs, le rapport soulignait que le temps pressait (1982:53)

"La création d'un réseau national de télécommunications doit fournir l'infrastructure nécessaire à l'épanouissement culturel et à l'expansion économique du Canada; elle exige que les organismes fédéraux et provinciaux concernés accordent une attention sérieuse à l'élaboration d'une politique des télécommunications.

Le rapport traite ensuite de la future politique canadienne des télécommunications (1982:53):

"Il faut que les autorités canadiennes élaborent sans tarder une politique détaillée des télécommunications, sinon la confusion qui en résulterait conduirait à un gaspillage des ressources, à une perte de temps dans la course mondiale à l'expansion des réseaux télématiques, et peut-être à la pénétration du marché canadien par des réseaux étrangers. Il est donc impératif d'adopter une telle politique, en répartissant les domaines d'activités entre les entreprises intéressées et en lui donnant quelque flexibilité pour tenir compte de la création éventuelle d'autres entreprises, et de l'apparition de technologies nouvelles."

Par le passé, et même plus récemment, le gouvernement a accordé une grande priorité à la souveraineté et à d'autres préoccupations non économiques dans le cadre de cette ère de l'information qui prend actuellement forme.

Quelles que soient les conséquences éventuelles de la TMD sur le Canada, les États-Unis ont récemment manifesté leur volonté de discuter

d'une libéralisation sectorielle du commerce, et notamment de l'informatique. Les deux pays étant engagés dans le système d'échanges multilatéraux du GATT, les ententes bilatérales doivent faire l'objet de négociations particulières. Les États-Unis ont demandé la coopération du Canada afin d'augmenter le volume du commerce et des investissements, d'abroger certaines mesures irritantes comme les dispositions obligeant les États-Unis à acheter des produits canadiens, de dissiper les incertitudes au sujet de l'accès à l'information, et d'abolir les barrières non tarifaires. Néanmoins, les récentes audiences du gouvernement des États-Unis au sujet de l'industrie de l'acier remettent en question leur engagement en faveur "du libre échange". Les quotas imposés par le gouvernement des États-Unis à l'importation d'autos japonaises constituent un autre exemple d'une approche fort peu "libre-échangiste", lorsque les États-Unis (ou leurs électeurs) estiment que leurs intérêts sont menacés.

Si l'on se contente du statu quo à l'égard de la TND, ou même d'un statu quo modifié, une politique sans plan d'ensemble ou une politique de simple augmentation aurait ultimement pour effet de placer les États-Unis dans une position favorable ou prioritaire et ce, pour deux raisons principales. Le premier motif tient à la rapidité d'intervention du gouvernement des États-Unis pour protéger ses intérêts acquis et à l'importance des moyens engagés; deuxièmement, une grande partie des institutions et des industries concernées par toute négociation sont soit étroitement interconnectées avec le marché des États-Unis, soit contrôlées par des sociétés-mères américaines. Par conséquent, si l'on se contente d'une approche sectorielle visant simplement à remédier aux dispositions irritantes ou à régler des litiges isolés, on assistera tout simplement à

un déclin graduel de la position canadienne à long terme. Ce commentaire vaut pour les trois grands domaines commentés ci-dessus, soit la protection des renseignements personnels, l'emploi et la souveraineté.

LES OPTIONS

Quelles sont alors les options qui s'offrent à nous? Si le statu quo, un statu quo modifié ou une politique d'accroissement ne sert pas l'intérêt national, quel autre type de mesures peut-on prendre? Nous pourrions étudier l'exemple du Brésil; il s'agit d'un modèle de type négatif, mais il vaut la peine d'être examiné afin de déterminer si ce modèle ou cette approche sont envisageables dans le contexte canadien. Après avoir décrit de façon relativement détaillée les mesures adoptées par le Brésil en réponse aux problèmes de l'informatique, de la protection des renseignements personnels, des ordinateurs et de la TMD, je formulerai une solution canadienne originale.

Le gouvernement brésilien ne veut pas devenir une "colonie informatique"⁴ et sa détermination a entraîné, au cours de la dernière décennie, la création d'un réseau complexe de règlements appliqués par le Secrétariat spécial à l'informatique. Le Brésil voit son indépendance dans le domaine de la technologie informatique comme une question de souveraineté et de fierté nationale; en outre, le gouvernement a adopté des mesures énergiques afin d'assurer le développement d'une forte industrie nationale de l'informatique. Ce facteur nationaliste s'était déjà manifesté lors de la naissance de l'industrie informatique brésilienne quand, au milieu des années 70, le ministère de la Marine de ce pays exigea

des mesures de sécurité pour l'installation des systèmes informatiques dans ses frégates et destroyers. Le projet fut donc entièrement confié au Conseil de la sécurité nationale du gouvernement militaire. En 1977, celui-ci parraina la création d'une compagnie d'informatique étatisée (Cobra), et établit deux ans plus tard le Secrétariat spécial à l'informatique, dirigé en grande partie par des ingénieurs de l'armée et de la marine.

Depuis lors, un groupe composé d'officiers de l'armée, d'entrepreneurs locaux et de nationalistes culturels de gauche s'est rallié à la cause de la protection de la croissance de l'industrie informatique brésilienne naissante. La part totale du marché détenue par les filiales de sociétés étrangères, et surtout I.B.M.⁵, a décru. En cinq ans, leur part du marché est tombée de 77 à 53 pour cent. Depuis 1979, les ventes d'ordinateurs fabriqués au Brésil sur le marché intérieur sont passées de 200 millions à près de 700 millions de dollars. Les ventes d'ordinateurs importés ont chuté d'un maximum avoisinant les 300 millions de dollars en 1981, à moins de 100 millions de dollars en 1983.

Le congrès brésilien débat actuellement une loi régissant les grandes orientations dans le domaine de l'informatique, en outre, le gouvernement veut éliminer la confusion résultant de la réglementation pléthorique visant les cas particuliers. Quelle que soit la décision prise par le gouvernement brésilien, les chiffres indiquent que le blocage des importations a contribué au succès de l'industrie locale. Les mesures énergiques adoptées par le gouvernement ont assuré le développement d'une industrie nationale de l'informatique. Les véritables perdantes sont les sociétés multinationales étrangères.

Il y a également eu d'autres activités.

Sur le plan international, l'OCDE a adopté les "Lignes directrices régissant la protection de la vie privée et la transmigration des données personnelles" (sept. 1980). Le Conseil de l'Europe a adopté une "Convention sur la protection de la vie privée des individus à l'égard du traitement informatisé des données personnelles." En ce qui concerne la TMD des renseignements non personnels, environ 60 pays ont émis une déclaration officielle quelconque selon le Centre des sociétés transnationales.

Un autre exemple est celui de la Suède, dont la Commission de l'inspection des données fonctionne depuis 1974. Les banques de données contenant des renseignements sur les activités des citoyens ne peuvent être consultées sans la permission de "l'inspectorat". Si des renseignements personnels doivent être utilisés hors de Suède, on ne peut les obtenir qu'avec une permission spéciale.

La tendance vers une réglementation accrue au sujet des données, particulièrement en Europe, aura indirectement en dernière analyse des conséquences sur la TMD dans les autres pays.

TABLEAU 1

1. Protection des renseignements personnels
Règlements et problèmes
2. A. Type de règlement
B. Personnes protégées - personnes naturelles; citoyens/résidents
seulement;
personnes morales
C. Données identifiables par les noms -- TÊD/TAB
Traitement manuel des données; collecte/flux/stockage
D. Contrôle - Commissions de contrôle des données
Enregistrement/Permis
E. Droit d'accès/de contestation
Liberté de l'information
F. Palier de gouvernement - Local, national, international
G. Secteur réglementé; public, privé, auto-réglementation
H. Mesures d'application; amende, indemnisation des victimes,
confiscation/destruction des données
2. Pays: Australie, Autriche, Belgique, Canada, Danemark, Finlande
France
Hongrie
Islande
Israel
Japon
Luxembourg
Pays-Bas
Nouvelle-Zélande
Norvège
Portugal
Espagne
Suède
Suisse
Royaume-Uni
États-Unis
Allemagne de l'Ouest

CEE
CE
OCDE
BII
3. Note: Le niveau de "réglementation" ou la sévérité des lois et de leur application varie selon les pays étudiés. Un "X" signifie simplement qu'il existe une condition, mais ne dit rien de sa sévérité.

Source: Transnational Data Report, 1978-1983, vol. 1 à 6; CEE, CE, Rapports du BII, Lignes directrices de l'OCDE, et correspondance personnelle.

Tableau 1: Réglementation sur la transmigration des données, sur la protection des données et sur la protection de la vie privée dans 22 nations.

Un Pacte continental sur les communications (PCC):

Les rapports, études et commissions qui ont essayé de s'attaquer aux problèmes de la TMD n'ont pas permis d'identifier de stratégies claires pour le Canada. Les problèmes de protection de la vie privée, de concurrence, de changements technologiques et de la réglementation multilatérale viennent compliquer encore plus l'adoption d'une politique. Pour remédier efficacement au problème de la TMD de façon plus réaliste, il est nécessaire de le scinder sous une forme plus malléable, par exemple un accord bilatéral unique avec le partenaire commercial le plus important du Canada, les États-Unis.

L'approche utilisée pour élaborer une politique au sujet de la TMD dépend de plusieurs postulats fondamentaux. Le Canada est convaincu qu'il peut retirer d'énormes avantages d'un accroissement de la TMD. Certains observateurs ont suggéré que s'il veut profiter des occasions offertes dans cette industrie, le Canada doit élaborer une politique des télécommunications afin de pénétrer les puissants réseaux qui se font concurrence aux États-Unis. Des interruptions des flux de données entre nos pays pourraient avoir des conséquences négatives pour l'industrie des services informatiques et pour la quasi-totalité de l'activité industrielle au Canada. Celui-ci doit résister à la tentation du protectionnisme, afin d'assurer la fluidité des échanges de données, d'information et de services connexes. Nous ne voulons pas devenir le Brésil du nord.

S'ils concluent un "Pacte continental sur les communications" (PCC), le Canada et les États-Unis seraient bien avisés de s'inspirer du Pacte de

l'automobile de 1965. Cet accord a été signé afin d'abolir les droits payables sur les échanges commerciaux entre manufacturiers américains et canadiens d'automobiles et de pièces détachées. Au moment de la signature du Pacte, le Canada était en position de faiblesse dans l'industrie de l'automobile; il était incapable de soutenir la concurrence sur le marché international en raison des frais qu'il fallait engager pour copier les voitures américaines dans les filiales canadiennes. Le Pacte de l'automobile promettait de redresser le déficit de la balance commerciale dans ce secteur et de faire augmenter la production au Canada.⁶

Au cours de récentes discussions sur les relations économiques entre les États-Unis et le Canada, l'adjoint suppléant du secrétaire d'État, M. James Medas, a souligné que le gouvernement Reagan est fermement déterminé à promouvoir une plus grande libéralisation du commerce. Le mois dernier, le Canada et les États-Unis ont signé une entente assurant les parties d'une consultation et d'une coopération rapides à l'égard des questions commerciales d'intérêt commun. Tout est maintenant en place pour la conclusion d'un PCC. Le gouvernement des États-Unis a identifié divers secteurs, dont l'informatique, qu'il envisageait dans le cadre de la récente initiative canadienne sur le libre échange sectoriel.

Étudions maintenant le PCC de façon plus approfondie.

Tout d'abord, le PCC concernera la télédiffusion, les télécommunications et les services et fournitures informatiques.

Deuxièmement il portera sur l'établissement d'un réseau continental de communication auxquels participeront les gouvernements nationaux des États-Unis et du Canada.

Troisièmement, les parties ayant des intérêts en jeu (les intervenants publics et privés, y compris les gouvernements provinciaux) devraient être consultés avant la conclusion d'un PCC.

Qui sont au juste ces parties. La liste suivante en donnera une idée:

- . Les entreprises d'informatique
- . Télésat Canada
- . TCTS et CNCP
- . Les compagnies provinciales de téléphone
- . Les compagnies de distribution par câble
- . Les producteurs cinématographiques indépendants
canadiens/Téléfilm
- . Les magazines nationaux
- . Les fournisseurs et fabricants de matériel, p. ex. Mitel,
Northern Telecom, NABU, etc.
- . Les fournisseurs de logiciels - les fournisseurs d'information,
p. ex. Infoglobe
- . Les distributeurs de télévision à péage
- . Les annonceurs
- . Le milieu financier
- . Les investisseurs

- . Les gouvernements; les ministères fédéraux et provinciaux concernés
- . Les syndicats.

Une brève explication s'impose: nous disposons à l'heure actuelle d'une série de politiques sans plan d'ensemble, pensées à court terme et qui se contredisent fréquemment. En outre, le gouvernement fédéral omet souvent de tenir compte du rôle ou du point de vue des provinces lors de ses interventions.

Pendant ce temps, les satellites de diffusion, le câble, le vidéotex, la radio mobile et la TMD connaissent, sur le plan continental une croissance qui fait surgir des questions de principe étroitement reliées. Le PCC élargirait le marché des produits canadiens - matériel et logiciels - de façon à ce qu'il ne soit pas inondé par des produits étrangers, pour la plupart en provenance des États-Unis. On pourrait aider les services canadiens et redresser le déséquilibre actuel en négociant la diffusion des émissions de la Société Radio-Canada et du réseau CTV sur tous les réseaux de câble des États-Unis, ou la diffusion des nouveaux services à péage par les satellites de ce pays. En outre, le Pacte fournirait des lignes directrices aux compagnies canadiennes de distribution par câble comme Rogers, Maclean-Hunter, Cablecasting, etc. possédant des franchises aux États-Unis. Les émissions des réseaux américains sont diffusées sur les systèmes de câble canadiens et les services à péage des États-Unis sont reçus par un nombre croissant de stations terrestres basées au Canada (TVRO); la question principale

consiste maintenant à se demander pourquoi l'on ne pourrait pas conclure un accord réciproque afin d'en faire profiter les fabricants et les vendeurs de logiciels canadiens.

Le déficit commercial dans le matériel informatique et de bureau indique bien que le Canada doit conclure un pacte sur les communications. M. Chevreau (1983:B 5) indique que le déficit commercial du Canada a dépassé le niveau des 2 milliards de dollars en 1982; les exportations représentaient 890 millions de dollars tandis que les importations d'ordinateurs s'élevaient à 3 milliards de dollars. Malgré les efforts consentis par le gouvernement en vue de réduire le déficit par les ventes de Telidon ou de Office Communications Systems, la Société Evans Research Corp. de Toronto prédit que le déficit passera à 5 milliards de dollars en 1986. La tendance vers l'automatisation des bureaux a fait augmenter la demande canadienne de matériel électronique de bureau étranger. Les quelques dollars injectés par le ministère des Communications dans des projets de bureautique ne font que masquer les problèmes fondamentaux plus graves de nature structurelle.

La vente d'émissions canadiennes aux États-Unis suscite plus d'espoirs, quoiqu'on n'ait pas encore établi l'existence d'une telle demande. Selon le rapport annuel de la société Radio-Canada (1981-1982), il semble exister un marché pour les produits canadiens, particulièrement dans le domaine des arts, outre celui des émissions d'information, As It Happens et Sunday Morning. Celles-ci ont établi un précédent laissant entrevoir la possibilité d'une présence canadienne plus importante sur la scène américaine des communications. Un pacte sur l'information

permettrait d'exposer la stratégie de promotion des productions de la SRC, de l'ONF, de la SDICC ou de Téléfilm sur les réseaux et les écrans américains.

En ce qui concerne la technologie des satellites, le Canada est obligé de conclure un pacte avec les États-Unis au sujet des services futurs de radiodiffusion par satellite. Le Canada et les États-Unis essaient tous deux de réserver des positions orbitales de choix afin d'y installer plus tard des satellites. La CFC envisage d'établir un système de radiodiffusion par satellite pouvant transmettre jusqu'à 13 services, et le Canada demande six positions orbitales avec une largeur de bande de 500 mhz à pleine fréquence réservée pour chaque service. La demande du Canada soulève le problème de la séparation maximale entre chaque satellite qui sera nécessaire pour répondre aux besoins des services canadiens proposés; cela signifie également qu'il ne restera aux États-Unis que 4 positions orbitales, pour la plupart peu avantageuses. Il sera nécessaire de rajuster les demandes des deux pays dans le cadre des négociations; les États-Unis préconisent cependant un système où les requêtes sont accordées sur demande, le premier arrivé étant le premier servi.

Et pourtant, une fois de plus, le Canada fait preuve de sa détermination à préserver sa souveraineté en demandant une position orbitale pour chacun de ses cinq fuseaux horaires, et une position supplémentaire destinée à la programmation française pour le Québec. Le Canada ne possède pas les ressources économiques pour mettre immédiatement ces services en oeuvre, mais il essaie d'empêcher les États-Unis de

s'approprier dès maintenant toutes les positions disponibles. (On doit se souvenir que d'autres pays importants, notamment en Amérique du Sud, espèrent utiliser à l'avenir les services de radiodiffusion par satellite, et gardent l'oeil tourné vers les zones de l'espace que le Canada et les États-Unis espèrent s'approprier.)

Un autre exemple de ce mouvement informel vers la conclusion d'un PCC est l'accord récemment conclu par le ministère des Communications et la NASA en vue de définir un programme spatial commun, permettant de répondre aux besoins des communications mobiles dans les deux pays. Cet effort pourrait aboutir à l'établissement d'un système de satellites mobiles offrant des services semblables dans les deux pays.

Les questions relatives au contenu et à l'origine du matériel et des logiciels pourraient toutes deux être abordées dans le cadre des négociations sur un satellite conjoint desservant à la fois les publics américain et canadien. La stratégie canadienne à cet égard devrait prévoir une entente bilatérale avec les États-Unis portant sur les points suivants: un partage des revenus tirés du réseau de satellites commun; un partage équitable en ce qui a trait au contenu des émissions et aux moyens de télécommunication; un partage équitable des services de programmation américain et canadien assurés par le satellite; et un partage de la recherche et du développement. Ce dernier aspect évitera au Canada de devenir un serf technologique à l'ère de l'information.

Mentionnons un dernier point. La proposition d'un PCC vise le renforcement des industries culturelles canadiennes; le statu quo oblige

les auteurs, les producteurs, les réalisateurs, etc. à diluer continuellement les références, les histoires, les thèmes, etc., canadiens afin de s'adapter aux exigences commerciales des États-Unis. La diffusion serait garantie par la conclusion d'un PCC, et il sera alors possible de véhiculer un point de vue spécifiquement canadien, inspiré d'idées, de normes et de perspectives, etc., canadiennes (comme le fait l'industrie cinématographique australienne). Le PCC ne vise pas la diffusion auprès d'un auditoire de masse, mais s'inscrit plutôt dans l'approche de diffusion restreinte, adoptée dans le cadre des systèmes mixtes nord-américains (câble-satellites) actuellement en pleine évolution.

S'il ne mène pas à terme une entreprise audacieuse comme le PCC, le Canada perdra sa position déjà faible dans le domaine de la technologie du matériel et des logiciels. Le statu quo constitue en fait une politique à courte vue, le Canada étant assuré en ce cas de perdre sur tous les tableaux (matériel et logiciels). Des politiques ponctuelles ne suffisent pas à assurer une présence canadienne importante sur la scène internationale et continentale, et les forces du marché ont toujours démontré que la programmation américaine bénéficie d'une avance considérable sur les productions canadiennes. Il devient donc de plus en plus urgent de conclure un PCC avec les États-Unis, et il appartient aux responsables canadiens chargés de définir les grandes orientations d'explorer les avenues existantes, afin de garantir la souveraineté canadienne, d'assurer la protection des renseignements personnels des Canadiens et de leur ouvrir des possibilités d'emploi à l'ère de l'information.

CONCLUSIONS

En résumé, dans ce document, nous avons étudié en partie la question de la TMD à travers le prisme de la protection de la vie privée, en nous arrêtant également aux problèmes de l'emploi et de la souveraineté nationale. Nous avons également commenté trois types d'approche à l'égard des mesures qui devraient être prises à l'avenir dans le domaine de la TMD.

En premier lieu, nous avons étudié l'option du statu quo, ou d'un statu quo modifié, qui entraînerait avec le temps une détérioration de la position canadienne en faveur de la position du gouvernement des États-Unis, et à l'avantage des intérêts commerciaux et corporatifs des industries de la communication aux États-Unis.

Deuxièmement, nous avons étudié un modèle restrictif de TMD, notamment celui du Brésil, en exposant les motifs justifiant les mesures prises par ce pays dans le domaine de l'informatique.

Troisièmement, nous avons exposé un plan original et donné plus de détails sur un Pacte continental sur les communications (PCC). Nous avons identifié les divers intérêts en jeu, soit les entreprises de radiodiffusion, de télécommunication et d'informatique. En outre, nous avons illustré la variété des problèmes par des exemples; nous avons indiqué une possible approche procédurale faisant appel à la participation des secteurs publics et privés, et à celle des gouvernements provinciaux. Enfin, nous avons exprimé l'avis que le PCC permettrait à la fois d'affirmer et d'enrichir la souveraineté culturelle du Canada en tant

qu'état-nation, qu'il assurerait une distribution plus équitable de la recherche et du développement dans les technologies futures de la communication et qu'il améliorerait les possibilités de création d'emplois du secteur secondaire dans le domaine de la haute technologie au Canada.

NOTES

1. Aux fins du présent document "La transmigration des données peut être définie comme la transmission de données et d'information pouvant être lues par une machine, par l'intermédiaire d'ordinateurs transnationaux et d'autres systèmes électroniques de communication, à des fins de stockage, de recherche ou de traitement." "Transborder Data Flow, Informatics, and National Policies", Journal of Communication, hiver, 1984, p. 154.
2. La déclaration de l'OCDE au sujet des données sera discutée à Paris les 2 et 3 juillet 1984 par le groupe de travail de l'OCDE sur la TMD.
3. Il est quelque peu paradoxal de constater qu'en 1984, la nation la plus impliquée dans les affaires internationales relatives à la communication - les États-Unis - est également celle qui s'efforce le plus activement de freiner les organisations ou associations internationales les plus susceptibles de l'aider à atteindre ses objectifs, qu'il s'agisse de la liberté des échanges de l'information, de la TMD, de la liberté du commerce, ou de l'utilisation rationnelle et efficace des fréquences radio-électriques au plan international. Citons par exemple le passage suivant qui accuse le gouvernement Reagan d'adopter une approche nuisible, néfaste et négative dans les grandes orientations des États-Unis et leur participation aux affaires internationales en cette matière:

"Les États-Unis à l'écart

Au contraire, les États-Unis prennent l'orientation inverse, abandonnant ou neutralisant un forum où peuvent échanger les

représentants d'un auditoire vaste et varié, et susceptible de s'adapter aux conditions changeantes et à de nouvelles perspectives. Les États-Unis menacent de se retirer de l'UNESCO, en partie à cause de l'attention que celle-ci porte aux pratiques et aux conditions des télécommunications internationales. Les États-Unis font pression sur l'Union internationale des télécommunications (UIT) elle-même, afin que celle-ci limite son action à des considérations techniques. Ils réduisent leur participation au Comité des Nations Unies sur l'information et aux sous-comités juridiques et techniques qui étudient les communications spatiales de l'avenir pour le Comité sur les utilisations pacifiques de l'espace. Les États-Unis prennent leurs distances face au Bureau intergouvernemental sur l'informatique et au Centre des Nations Unies sur les sociétés transnationales, qui manifestent tous deux un très grand intérêt pour les problèmes de transmigration des données impliquant le tiers-monde." Chronicle of International Communication, avril 1984, volume 5, numéro 3, page 7.

4. On trouvera les commentaires détaillés dans: T.L. McPhail, Electronic Colonialism: The Future of International Broadcasting & Communication, (Beverly Hills, Californie: Sage Publications, 1981). Voir également les autres ouvrages du même auteur énumérés dans la bibliographie.

5. La société I.B.M. a également été critiquée aux États-Unis mêmes.

"De plus, la société I.B.M. a récemment démontré qu'elle n'hésiterait pas à intenter des poursuites contre ses adversaires, même mineurs; cela a tempéré l'ardeur de ses concurrents potentiels, surtout s'il s'agit

d'anciens employés, d'I.B.M. On risque d'assister à la création d'une classe de "serfs technologiques", qui ont travaillé à un moment donné pour I.B.M. et qui sont maintenant perpétuellement exposés à des poursuites pour violation de secret commercial. C'est un paradoxe inquiétant: maintenant libérée des poursuites que lui avait intentées le gouvernement (des É.-U.), I.B.M. utilise des recours judiciaires pour restreindre la concurrence et bloquer la diffusion de la technologie, particulièrement dans le domaine des gros ordinateurs directement connectables" New York Times, dimanche, 13 mai 1984, page 2F.

6. Je ne commenterai pas ici les détails ou les résultats du Pacte de l'automobile, mais M. Beigie (1970) et d'autres auteurs ont réalisé des études sur ce sujet.

Références:

Beigie, Carle E. "The Canada-U.S. Automotive Agreement: An Evaluation."
Canadian American Committee, Canada. 1970.

"Brazil's Prickly Computer Policy". The New York Times, avril 29, 1984.
p. 12F.

Chevreau, Jonathan, "Computer, Office Equipment Showing Higher Trade
Deficit." Globe and Mail, février 11:B5, 1983.

Clyne, J.V. "Le Canada et la télécommunication, Comité consultatif des
télécommunications et de la souveraineté canadienne." Ministère des
Approvisionnement et Services, Canada. 1979.

"Council of Europe Convention for the Protection of Individuals with Regard
to Automated Processing of Personal Data." Transnational Data Report 3(6),
1980.

Crawford, Morris H. "The IBI Transborder Data Flow Conference: An
American View." Transnational Data Report 3(3-4), 1980, pp. 38-41.

Cundiff, W.E. et Mado Reid, "Issues in Canadian/U.S. Transborder Computer
Data Flows." Institute for Research on Public Policy, Toronto:
Butterworth & Co. Canada, Ltd. 1979.

European Communities, Commission. "European Society Faced with the

Challenge of New Information Technologies: A Community Response."

Brussels: European Economic Community, 1979.

"Europe/North America: A One-Way Flow." Information Systems 30, 1979.

Ganley, Oswald G., "The United States-Canadian Communications and Information Resources Relationship and Its Possible Significance for Worldwide Diplomacy." Program on Information Resources Policy, Working Paper, Cambridge, Mass.: Harvard University, 1979.

Hamelink, Cees J. "Informatics: Third World Call for New Order." Journal of Communication 29(3), été 1979, pp. 144-148.

The Impact of Transnational Data Flows on Developing Countries. J.C. Grant. An address to the Conference on Information, Economics, and Power North South Dimension. The University of Western Ontario, School of Journalism. 10 mars 1984.

Instant World, "A Report on Telecommunications in Canada", Ottawa: Information Canada, 1971.

Issues in Canadian/U.S. Transborder Computer Data Flows. W.E. Cundiff and Mado Reid (Eds.) Proceedings of a conference sponsored by the Institute for Research on Public Policy. 1978.

Lesser, Barry, "The Implications of the Federal and Provincial Proposals for Regulating Telecommunications: An Economist's Perspective, in

Telecommunications Regulation and the Constitution.", Robert Buchan, Christopher Johnston (Eds.). Montreal: The Institute for Research on Public Policy. 1982.

Lester, R.M., "Communications and Transborder Information flows." Conference Board du Canada, Business Outlook Conference; document non publié, 1981.

Levine, H., & Rumberger, R. Stanford University, Project Report No. 83-A 4.

McPhail, Thomas L., "The Future of Canadian Broadcasting: Proposed Revision of Regulatory Mechanisms and Policies", in The Crisis in Canadian Broadcasting. (Ottawa: Canadian Broadcasting League, 1976).

McPhail, Thomas L., Electronic Colonialism: The Future of International Broadcasting and Communication. (Beverly Hills, Calif.: Sage Publications, 1981), pp. 259.

McPhail, Thomas L., "Telematics, Telejournalism in Public Policy Concerns", Competition in the Information Economy, Horizon House, 1981, pp. 417-420.

McPhail, Thomas L., "The Future of Canadian Communications", Communications in Canadian Society, B. Singer, (ed.) Toronto: Addison-Wesley 1983, pp. 73-82.

McPhail, Thomas L., "Direct Broadcast Satellites: The Demise of Public and Commercial Policy Objectives", Telecommunications in the year 2000:

National and International Perspectives, (S. Judge), Indu Singh, (ed.)
(Ablex Publishing Corporation, Norwood, New Jersey, 1983), pp. 72-79.

Medas Points directions in U.S./Canada Economic Relations. James Medas,
U.S. Deputy Assistant Secretary of State. Texte du discours prononcé à
Montréal, devant le Club Canadien de Montréal, Chambre de Commerce du
District de Montréal, et le Montreal Board of Trade. 19 mars 1984.

Melody, William, "Are Satellites the Pyramids of the 20th Century?" In
Search, volume VI, No. 2, printemps, pp. 2-9.

Organization for Economic Cooperation and Development. Guidelines on the
Protection of Privacy and Transborder Flows of Personal Data. Paris:
OCDE, 1981.

Préparons la société informatisée. Demain, il sera trop tard. Conseil des
sciences du Canada - Comité sur les ordinateurs et les communications.
1982.

Read, William H. "Foreign Policy: The High and Low Politics of
Telecommunications." In Anthony G. Oettinger, Paul J. Berman, and William
H. Read (Eds.) High and Low Politics: Information Resources for the '80s.
Cambridge, Mass.: Ballinger, 1977.

Robinson, Peter. "Some Economic Dimensions of TDF." Transnational Data
Report 3(3-4), 1980, pp. 18-19.

Schiller, Herbert I. "Computer Systems: Power From Whom and From What?"

Journal of Communication 28(4), automne 1978, pp. 184-194..

Conseil des sciences du Canada, Préparons la société informatisée: Demain il sera trop tard. Ministère des Communications, Ministère des Approvisionnementnements et Services, Ottawa, 1980.

Serafini, S. et M. Andrieu, "The Information Revolution and Its Implications for Canada." Ministère des Communications, Ministère des Approvisionnementnements et Services, Ottawa, 1980.

Silverman, Paul E. "The Evolving Market for International Communications." Telecommunications, avril 1978, pp. 25-30.

"Survey Shows 35 Countries to Regulate Data Flows." Transnational Date Report 1(7), 1978.

Telecommunications and Canada. Consultative Committee on the Implications of Telecommunications for Canadian Sovereignty

"Trade Barriers to Telecommunications, Data and Information Services."

Transnational Data Report 5(40), 1982, pp. 179-185.

Traded Computer Services: A Bilateral Beginning. Discours de Rowland C. Frazee, Président et Directeur Exécutif, Banque Royale du Canada, prononcé devant la Bookings Institution Washington, D.C. 10 avril 1984.

Transborder Data Flow a Hot Issue. Lawrence Surtees, Globe and Mail, 24 février 1984.

Transborder Data Flows: A Multinational Issue. C.J. Maule. Article paru dans Foreign Investment Review, automne 1982.

Trubow, George B. "Privacy, Policy and Computers." Document présenté lors du Computer Privacy and Security Symposium, "Top Secrets 1981," parrainé par Honeywell Information Systems, Inc., Phoenix, Arizona, avril 1981.

Wigand, Rolf T. "Direct Satellite Broadcasting: Selected Social Implications." In M. Burgoon (Ed.) Communication Yearbook 6. Beverly Hills, Cal.: Sage, 1982, pp. 250-288.

Wigand, Rolf T., Shipley, C. & Shipley, W., "TBDF, Informatics, & National Policies", Journal of Communication 24(1), hiver 1984, pp. 153-175.

Williams, J.K. "European Data Protection - A Business Viewpoint."
Transnational Data Report 5(3), 1982, pp. 156-157.

CA1

DOCUMENT: 870-123/008

74

- C02

INTERPROVINCIAL CONFERENCE ON PRIVACY:
INITIATIVES FOR 1984 (SYMPOSIUM)

Notes for Conference

Ralph Hancox
The Reader's Digest Association (Canada) Ltd.



Toronto, Ontario
May 23-24, 1984

Notes for

Conference on Privacy: Initiatives for 1984

Symposium

by Ralph Hancox

The Reader's Digest Association (Canada) Ltd.

for delivery May 23, 1984 at 2:30 p.m. at Private Sector Panel

What the Private Sector Has Done

Mailing lists and direct mail marketing.

At the outset, it might be useful, to put the privacy issue into perspective so far as direct mail marketing and mailing lists are concerned.

Unsolicited mail has a high profile in some quarters and, according to various indignant consumer protection spokesmen who have voiced opinions on the subject, a high irritation factor also.

Of the total mail volume delivered by Canada Post in recent years - about six billion, four hundred million pieces annually - some fifty percent, or three billion two hundred million pieces, fall into this category.

This approximates an average of a little less than two pieces of unsolicited mail (including bills) per household per delivery day. It is axiomatic that Canada Post would like to increase this average since this class of mail is, by virtue of its pre-sorted, batched characteristics, the most profitable kind of mail packet to handle.

It should also be said that, in Canada, direct mail marketing is an undeveloped sales technique. In a comparison with the United States our volumes are easily less than one twentieth of theirs per capita.

A variety of countries have tested public opinion on the subject of intrusion by mail and, it is true, there is a portion of the general public that would class unsolicited mail as an 'invasion of privacy'.

This small body of opinion also responds favourably to the sobriquet 'junk mail' which is applied by critics to undressed mail packets.

But when the privacy issue of mail delivery is tested on the spectrum of substantive privacy issues such as:

Would you regard it as an invasion of privacy if:

- one department of government made personal data from your file available to another government department?
- you were required to carry an identification card bearing your social insurance number?
- your neighbour allowed her dog to defecate on your lawn?
- you were regularly approached by door-to-door sales personnel to buy unsolicited merchandise?
- you were asked to supply personal information over the telephone to a caller not known to you?

unsolicited mail as a privacy issue becomes of negligible concern.

Similarly, on the question of mailing lists and the renting of names (which has been criticized in some quarters as an invasion of consumer privacy) public indignation - which in any case has never been high on this subject in North America - becomes inconsequential in the face of such questions as:

Who would you wish to intercept, or prevent the delivery of, unsolicited commercial mail destined for delivery to your household:

- the government?
- the post office?
- an independent agency?
- an industry association?
- the police?
- a privacy commissioner?
- none of these?

Would you prefer to do it yourself?

When the question is asked:

Would you object if a

- charitable organization,
- commercial enterprise,
- local merchant,
- direct mail marketing organization,
- magazine publisher,
- social club,
- health and fitness organization,
- government department,

took your name and address from a telephone directory

to solicit your support,
to ask for a donation,
to offer goods or services for sale,
to distribute information?

the answer reveals a very low level of anxiety in respondents about mailing lists.

It goes without saying that the weight of these answers can be very rapidly altered by phrasing questions to introduce the concept of the direct mail marketing, or delivery, of pornographic or other material generally regarded as offensive or unsolicited material to children.

There is a further change of attitude when the unknown mailer uses information which is quite clearly personal in nature.

'In your garage you have a brand new Ford ... would you like a set of seat covers....'

'You, your husband and three children will be delighted with....'

Such approaches immediately raise the questions:

'How did they know...?'

'Where did they get my name and address...?'

Those who compile mailing lists, and those who send unsolicited sales promotions to addresses on such lists, have a common interest in limiting and guaranteeing the information involved.

Such lists should contain up-to-date addresses - that is to say, people on them should be at the address stated. They should also be among those who have a high probability of responding to unsolicited mail. They should not contain names and addresses of people who object to unsolicited mail, or who have died.

It is expensive to plan, direct and control a mail marketing campaign. The efficiency of the response levels is crucial to profitability.

Thus mailers share with recipients a desire not to send mail to those who genuinely do not want it. (The question of sending unsolicited merchandise and then billing for it is, of course, another question already covered in consumer legislation.)

The question, always, for the mailer is how to avoid sending material to those who will never respond.

One way of increasing the probability of response and increasing response levels of mailing lists is to compile historical information on buying patterns and preferences of individuals on that list and to code lists with demographic and other sociographic information.

Such information can be weighted and regression formulas can be applied to name selection. In such a process, each name on the list to be regressed would receive a score. Only those names whose scores exceed a certain level would be selected from the list to mail.

The more accurate the regression, the more closely a direct mail marketing campaign can approach the nirvana of mailing only to those who respond favourably.

In fact, as the state of the art now is, a reasonable response level is a low percentage, normally well below ten percent. An acceptable improvement from regression would be a one percent or even .75 percent increase in response.

The percentage of respondents, depending on a variety of factors, may be always in that order of magnitude for a particular list, but the individuals in that list who respond on successive occasions will be randomly distributed throughout the universe and may seldom respond twice to repeated mailings.

The notion, therefore, that direct mailers can - or would want to - make sinister use of information on mailing lists, or any use except to increase the response level, is highly fanciful.

The issue of intrusion is also raised in discussions of unsolicited mail and, should, perhaps, be disposed of in this attempt to set the perspective.

Direct mail marketing is, among selling methods, a low pressure sales technique, the initiative for which, after the first mailing piece has been dispatched, is always in the hands of the buyer. Consider the following:

A potential customer receives a mailing piece. The customer can decide to open the envelope or discard it.

If the customer opens the envelope, the contents will either prompt an order or be discarded.

If the customer places an order, the order must be put in an appropriate envelope, be stamped and be mailed, giving time for further reflection.

If the order is mailed, the customer will receive the goods ordered and may accept them, hold them for a trial period or return the goods to the merchant.

Then, of course, comes the task of billing and payment. The merchant trusts and prays that the payment response level matches the original response level for orders.

Three points are of interest to conclude this part of the discussion:

1. In places where an opportunity exists for consumers to remove their names from mailing lists, not many people do so (in Canada, some 27,567 people or some .34 percent of the active households have registered with the Canadian Direct Marketing Association for this purpose).
2. Significantly more people ask to be put on mailing lists than ask to be taken off in the American experience.
3. The trading of mailing lists which are up-to-date and which are marked with data already in the public domain - such as address and postal code - is an economic benefit to the industry and the consumer. (So much so, incidentally, that a state advisory committee concluded in Illinois that 'the sale of driver license lists by a government unit to direct mail firms does not constitute an invasion of privacy' and that it should be encouraged by legislation.

That same committee made another point which neatly leads into the next body of issues to be considered.

In a discussion of whether applicants for a driver's license should have the option of excluding, by check-off, their names from the list that the State of Illinois could trade, the committee reported thus:

'We have examined the practical effects of granting an option... to preclude the Secretary of State from disclosing information as to applicant's name, address, date of birth, and other related information... The objective of the check-off would be to protect persons from the receipt of unsolicited mail. We find that the check-off would not achieve the objective sought... The likely result would be that the Secretary of State would be criticized for misleading persons and not preventing the delivery of unsolicited mail...'

This comment is very true. As the Australian Law Reform Commission found when it examined the whole issue of privacy in all its aspects. It quotes the following passage in support of its recommendations on mailing lists:

'If an individual does not want to receive unsolicited mail, he can keep his name off most lists by becoming a modern-day hermit - by paying cash for all his purchases, not owning a car, giving to charities anonymously, always buying magazines at newsstands, never responding to door-to-door surveys, never signing a petition or guest book, never registering to vote, never attending a meeting or conference, or newsworthy or social event... even so he may get a certain amount of unsolicited mail addressed to the occupant...'

Here, the author has chosen to interpret the individual as a male. We are all aware that, in the same household may live a male and a female who have differing views on whether that household, or one of the occupants of it, should be on, or off, mailing lists.

In the discussion of various legislative models contained in the discussion paper circulated at this conference the registration of mailing lists is reviewed.

When Sweden took this approach it expected registrations at barely one hundred such lists; its registration office, however, was swamped with applications for thousands.

This is very understandable. An enormous number of lists are compiled for the purposes of mailing information to various universes. Clubs do it, schools do it, even mothers and politicians do it.

And in a communal society, it is very desirable that we do do it because it is all part of the network of the free flow of information.

As we have already noted, it is in the interest of the commercial mailer to ensure, as far as is possible, that the names on the list to be mailed are favourably disposed towards the mailing, contain only information which will enhance the efficiency of that mailing, are up-to-date and are judiciously used.

In a study commissioned for the Council of Europe, John Braun made this observation:

'If it is accepted that the use of the mail is open to anybody -- list or no list -- and that what is relevant is the content of the mailing piece and not

the act of mailing, then the issue to be faced is one of detriment. Is there anything in the content of the mail which offends against fair trading, honesty, morality, taste or any of the many possible alternatives? If the respondent is misled or likely to be misled or defrauded or shocked by the nature of the communication, there is cause for intervention by the appropriate authority'.

In most jurisdictions, such matters are already covered in legislation or regulation. What is not always covered and which, in the growing opinion of observers, should not be, is the registration, content, or use of commercial mailing lists.

The reasons, most generally are those of cost and impracticability.

The further and most powerful reason, of course, is that the process of self-regulation is in the best interest of users, society and recipients, in any case.

This does not imply that there are no abuses and no weaknesses and no faults where self-regulation is applied. There are; but these can be shown to be far less than those which would occur and have occurred in legislatively regulated systems.

Consider, for example, the anomaly in a jurisdiction, where it would be illegal to publish the sex or political affiliation of members in a list of names and addresses of the constituents of a legislative assembly. This sort of thing is one of the hazards of an over-zealously worded privacy regulation.

Less far-fetched, but equally absurd, would be a requirement for clubs, say, to register their lists of members, and submit the information contained on such lists for approval, by club members. This regulatory precaution would be against the eventuality that the list might be rented or sold to a

commercial enterprise with a legitimate interest in mailing the people on it.

The Organization for Economic Cooperation and Development has published guidelines governing privacy protection where mailing lists are concerned and these have been widely embraced. The U.S. and Canadian Direct Mail Marketing Associations and marketing groups in European, British and Scandinavian countries have all adopted codes of conduct and it is of interest that such actions have taken place in countries where legislation is in place and where it is not.

Essentially, all these codes embrace the following principle and concepts contained in Reader's Digest's code.

1. Personal data collected and stored are limited to those relevant to the efficient marketing, order processing, servicing, billing and collection of payment for the company's products and services, and are used only for these purposes.
2. The personal data files are frequently updated with new information to ensure that they are accurate, complete and current.
3. Reader's Digest responds on a timely basis to written requests from Customers or other individuals (or their documented legal representatives) for summaries of their personal data in the file. Personal data shown to be inaccurate, obsolete, or incomplete are corrected.

4. Except for debt recovery purposes on behalf of Reader's Digest or when required by law, personal data are not released to third parties.
5. Strict security procedures are maintained to protect against unauthorized access, destruction, use, modification or disclosure of personal data on Reader's Digest Customers.
6. Reader's Digest supports efforts of industry associations to which it belongs to encourage the disclosure of list rental or exchange policies and the offer of a name removal option by companies who engage in those practices.
7. Reader's Digest honors on a timely basis all requests from those who do not wish to receive its promotional mailings by appropriate notation to the file. The requests may be received directly or through third parties, such as consumer and industry associations or government agencies.
8. Reader's Digest complies with all local laws and regulations relating to data protection and privacy.

Reader's Digest does not rent or trade the names and addresses of its customers, incidentally.

Progressive companies are increasingly adopting well formulated and responsible voluntary codes, which, if they contain such elements as those outlined in the Discussion Paper circulated for this meeting would render anything but an umbrella statute unnecessary.

Along these lines, the Australian Law Reform Commission, in its recommendations, has struck the right balance.

It is perhaps, worth repeating the essential elements of a worthwhile code on list management to bring this presentation to a close.

- Personal information should be obtained and processed fairly and lawfully;
- Personal information should be held for a specified and legitimate purpose or purposes;
- Personal information should not be used or disclosed in a way incompatible with those purposes;
- Personal information should be adequate, relevant, and not excessive in relation to the specified purposes;
- Personal information should be accurate and, where necessary, kept up to date;
- Personal information should be kept in name linked form for no longer than is necessary for the specified purposes;
- The data subject should have access to information held about him or her and be entitled to its correction or erasure where the legal provisions safeguarding personal data have not been complied with;

- Appropriate security measures must be taken against unauthorized access, alteration or dissemination, accidental loss and accidental or unauthorized destruction of data.

It is self-regulation that prompted the Australian law commission on reform to conclude:

'The commercial benefits arising from adoption of these methods (which I described earlier) by direct mailers (in particular, reduced cost of mailings improved returns, enhanced customer goodwill) provide motivation to members to pursue these schemes. This facilitates market advantages of the direct mailing system, which includes increases in sales of goods and services and expansion of employment proposals, while minimizing the number of people receiving unsolicited communications...'

CA1
Z4
-252

DOCUMENT: 870-123/008

Traduction du Secrétariat

CONFÉRENCE INTERPROVINCIALE SUR LA PROTECTION
DES RENSEIGNEMENTS PERSONNELS:
MESURES POUR 1984 (COLLOQUE)

Notes en vue d'une allocution



Ralph Hancox
The Reader's Digest Association (Canada) Ltd.

Toronto (Ontario)
Les 23 et 24 mai 1984

Notes en vue d'une allocution prononcée au colloque de la
Conférence sur la protection des renseignements personnels:
mesures pour 1984

par Ralph Hancox

The Reader's Digest Association (Canada) Ltd.

Le 23 mai 1984 à 14 h 30 à la réunion sur le secteur privé

Ce qu'a fait le secteur privé

Liste de distribution et commercialisation directe par courrier

Dès le départ, il serait peut-être utile de ramener la question de la protection des renseignements personnels à ses justes proportions dans la mesure où cela touche la commercialisation directe par courrier et les listes de consommateurs.

Le courrier importun fait beaucoup parler de lui dans certains milieux et, selon les divers défenseurs du consommateur qui ont exprimé leur indignation à ce sujet, il soulève également beaucoup d'exaspération.

Sur le volume de courrier total livré par Postes Canada ces dernières années (environ six milliards quatre cents millions d'envois annuellement), quelque 50 p. 100, ou trois milliards deux cents millions, s'inscrivent dans cette catégorie.

Ces chiffres représentent donc en moyenne un peu moins de deux envois de courrier importun (y compris les factures) par ménage par journée de livraison. D'ailleurs, Postes Canada aimerait bien augmenter cette moyenne car, en raison du fait qu'elle est déjà triée et en vrac, cette catégorie de courrier constitue la plus rentable qui soit à traiter.

Il convient également de souligner qu'au Canada la commercialisation directe par courrier est une technique de vente sous-développée. Par comparaison avec les États-Unis, le volume traité ici représente moins du vingtième de celui enregistré là-bas par personne.

Dans différents pays, on a évalué l'opinion publique sur la question des ingérences par courrier et, il faut l'admettre, il y a une partie du grand public qui considère le courrier importun comme étant une "ingérence dans la vie privée".

Cette petite portion de l'opinion publique considère également que les personnes qui critiquent les envois postaux non adressés ont raison de les considérer comme du "courrier - rebut".

Cependant, lorsque le respect de la vie privée par rapport à l'envoi du courrier est évalué d'après une gamme de questions fondamentales comme:

À votre avis, s'agirait-il d'une ingérence dans la vie privée si:

- o un ministère tirait de votre dossier des données personnelles pour les transmettre à un autre ministère du gouvernement?
- o vous étiez tenu de porter une carte d'identité portant votre numéro d'assurance sociale?
- o votre voisine permettait à son chien de faire ses besoins sur votre pelouse?
- o vous étiez régulièrement visité par des vendeurs itinérants sans que vous l'ayez demandé?
- o si un inconnu vous demandait de lui donner des renseignements personnels au téléphone?

le courrier importun en tant que menace à la vie privée devient alors une préoccupation bien secondaire.

De même, pour ce qui est de la question des listes postales et de la location de listes (méthodes qui ont été critiquées dans certains milieux comme étant une intrusion dans la vie privée du consommateur) l'indignation publique - qui de toute façon n'a jamais été très forte sur ce sujet en Amérique du Nord - devient négligeable face à des questions comme:

À votre avis, qui devrait intercepter le courrier commercial importun destiné à votre ménage, ou en empêcher la livraison,

- o le gouvernement?
- o le bureau de poste?
- o un organisme indépendant?
- o une association industrielle?
- o la police?
- o un commissaire privé?
- o aucun de ces intervenants?

Préféreriez-vous le faire vous-même?

Par ailleurs, lorsqu'on pose la question suivante:

Vous opposeriez-vous à ce que:

- o une organisation charitable,
- o une entreprise commerciale,

- o une organisation de commercialisation directe par courrier,
- o l'éditeur d'une revue,
- o un club social,
- o une organisation de santé et de conditionnement physique, ou
- o un ministère gouvernemental

tire vos nom et adresse d'un annuaire téléphonique afin de

demander votre appui
solliciter un don
offrir des biens ou des services à vendre
diffuser des renseignements,

les réponses montrent que les répondants s'inquiètent très peu des listes de distribution.

Il va sans dire que la pondération de ces réponses peut se modifier très rapidement par la formulation de questions qui font appel au concept de la commercialisation directe ou de la livraison par courrier de documents pornographiques ou autres généralement considérés comme importuns et nuisibles pour les enfants.

L'attitude change encore lorsque l'inconnu qui est à l'origine de l'envoi utilise des renseignements qui ont une portée clairement personnelle.

"Vous avez dans votre garage une voiture Ford de l'année ... aimeriez-vous avoir un ensemble de recouvrement de sièges ..."

"Vous-même, votre mari et vos trois enfants serez heureux d'apprendre que ... "

Pareille formulation soulève immédiatement des questions:

"Comment peuvent-ils savoir ...?"

"Où ont-ils pris mon nom et mon adresse ...?"

Ceux qui compilent les listes de consommateurs et ceux qui envoient de la publicité importune aux adresses indiquées sur ces listes ont un intérêt commun à limiter et à garantir l'information dont il est question.

Ces listes devraient renfermer des adresses à jour, autrement dit, les personnes mentionnées devraient être à l'adresse indiquée. Elles devraient également appartenir au groupe qui répondra très probablement au courrier impersonnel. Les listes ne devraient pas contenir le nom et l'adresse de gens qui refusent de recevoir du courrier importun ou qui sont décédés.

La planification, l'orientation et la surveillance d'une campagne de commercialisation par courrier coûte cher. La rentabilité du taux de réponse est donc essentielle.

Les expéditeurs et les récipiendaires ont donc en commun le désir de ne pas envoyer de courrier à ceux qui n'en veulent vraiment pas. (La question relative à l'envoi de marchandise importune qui est ensuite facturée constitue évidemment un autre point que visent déjà les lois sur la consommation.)

L'expéditeur essaie donc toujours d'éviter d'envoyer des documents à des gens qui n'y répondront jamais.

Une façon d'accroître la probabilité de réaction ainsi que les taux de réaction des destinataires tirés d'une liste de consommateurs consiste à compiler des données sur les modes d'achat et les préférences des personnes inscrites sur cette liste et de coter les listes en fonction de renseignements démographiques et d'autres données sociographiques.

Il est possible de pondérer ces renseignements et d'appliquer des formules de régression au choix des noms. D'après ce processus, chaque nom sur la liste à évaluer se voit attribuer des points et seuls les noms dont le pointage dépasse un certain niveau sont choisis comme destinataires

Plus le dosage est précis, plus les concepteurs de la campagne de commercialisation directe par courrier peuvent s'approcher de l'idéal d'une expédition qui ne s'adresserait qu'aux personnes qui y répondront favorablement.

En fait, dans l'état actuel des choses, le niveau de réponse raisonnable est un faible pourcentage, habituellement bien inférieur à 10 p. 100. Une amélioration acceptable de la formule serait représentée par une augmentation du taux de réponse de 1 p. 100 cent ou même de 0,75 p. 100.

Le pourcentage des répondants, qui varie en fonction de toute une gamme de facteurs, peut être toujours du même ordre pour une liste particulière, mais les personnes inscrites sur cette liste qui répondent à des appels successifs sont réparties au hasard dans l'univers et peuvent rarement répondre deux fois à des envois répétés.

Par conséquent, la notion selon laquelle les personnes qui expédient directement de la publicité par courrier ou qui veulent le faire sont prêtes à utiliser les renseignements donnés par ces listes pour servir de sombres desseins en vue d'accroître le taux de réponse relève de la plus pure fantaisie.

La question de l'ingérence dans la vie privée est également soulevée lors de discussions portant sur le courrier importun et il conviendrait peut-être de la mettre de côté afin de remettre les choses en perspective.

La commercialisation directe par courrier constitue, parmi les méthodes de vente, une technique qui exerce peu de pression et pour laquelle l'initiative revient, après le premier envoi, à l'acheteur. En effet:

Un client éventuel reçoit une lettre, il peut décider de l'ouvrir ou de la jeter.

Si le consommateur ouvre l'enveloppe et en lit le contenu, il peut ensuite soit faire une commande, soit ne pas tenir compte de l'offre.

Si le consommateur décide de faire une commande, il doit placer sa demande dans une enveloppe, la timbrer et la poster, ce qui lui donne le temps de réfléchir.

Après avoir posté sa commande, le consommateur recevra les biens qu'il a commandés et il peut les accepter, les conserver pendant une période d'essai ou les retourner au commerçant.

Puis vient le moment de facturer et de payer. Le commerçant espère de tout coeur que le taux des personnes qui payent correspond à celui des personnes qui ont répondu au départ.

Il convient de relever trois points intéressants pour clore cette partie de notre étude:

1. Là où les consommateurs ont la possibilité de faire rayer leur nom des listes d'expédition, très peu de gens le font (au Canada, quelque 27 567 personnes ou environ 0,34 p. 100 des ménages actifs se sont inscrits auprès de l'Association canadienne de la commercialisation directe par courrier à cette fin).
2. D'après l'expérience aux États-Unis, il y a beaucoup plus de gens qui demandent de faire inscrire leur nom sur les listes d'envoi que de le faire rayer.
3. L'échange de listes d'envoi à jour et dotées de données qui appartiennent déjà au domaine public, par exemple l'adresse et le code postal, représente un avantage économique pour l'industrie et le consommateur. (Cela est tellement vrai, entre parenthèses, qu'un comité consultatif d'État a conclu en Illinois que la vente par une unité gouvernementale de listes de personnes détentrices de permis de conduire à des entreprises de

commercialisation directe par courrier ne constitue pas une ingérence dans la vie privée et que cette formule devrait au contraire être favorisée par des mesures législatives.)

Le même comité a présenté un argument qui nous amène précisément aux questions que nous devons maintenant étudier.

En tentant de déterminer si les personnes qui demandent un permis de conduire devraient avoir la possibilité, en cochant une case d'exclusion, de soustraire leur nom de la liste que pourrait échanger l'État de l'Illinois, le comité déclarait:

(traduction non officielle)

Nous avons étudié les effets pratiques du fait... d'accorder la possibilité... d'empêcher le secrétaire d'État de divulguer des renseignements relatifs aux nom, adresse, date de naissance du demandeur et d'autres renseignements connexes... L'objectif de la case d'exclusion serait de protéger les personnes de l'envoi de courrier importun. Nous croyons que l'option d'exclusion n'atteindrait pas l'objectif recherché... Il en résulterait plutôt que le secrétaire d'État serait critiqué pour avoir trompé les gens et n'avoir pu empêcher l'envoi de courrier importun...

Cette observation est très juste. C'est d'ailleurs ce qu'a pu constater la Commission de réforme du droit de l'Australie lorsqu'elle a étudié l'ensemble de la question de la vie privée sous tous ses aspects. Elle cite le passage suivant à l'appui de ses recommandations au sujet des listes de distribution:

(traduction non officielle)

Si un homme ne veut pas recevoir de courrier importun, il peut éviter l'inscription de son nom sur la plupart des listes en devenant un ermite moderne - en payant comptant pour tous ses achats, en n'ayant pas de voiture, en faisant des dons anonymes aux oeuvres charitables, en achetant ses revues au comptoir, en ne répondant jamais aux enquêtes à domicile, en ne signant jamais de pétitions ou de livres d'invités, en ne s'inscrivant jamais pour voter, en n'assistant à aucune réunion ou conférence, à aucune réception sociale ou manifestation publique... et même là, il peut recevoir un certain volume de courrier importun adressé à l'occupant...

Dans l'exemple cité, l'auteur a choisi de supposer que la personne concernée était un homme. Or, nous savons tous que dans un même ménage peuvent vivre un homme et une femme qui ont des vues divergentes sur la question de savoir si le ménage, ou l'un de ses occupants, devrait être inscrit ou non sur des listes de distribution.

L'étude des divers modèles législatifs pertinents que renferme le document d'étude distribué à la présente conférence fait état de l'enregistrement des listes d'envoi.

Lorsque la Suède a adopté cette formule, elle s'attendait à ne recevoir qu'une centaine d'enregistrements; cependant, son bureau d'enregistrement a été inondé de milliers de demandes.

Cela est très compréhensible. Un nombre énorme de listes sont compilées aux fins de l'expédition de renseignements à divers groupes cibles. Les clubs le font, les écoles le font, même les mères de famille et les hommes politiques le font.

D'ailleurs dans une société communautaire, il est fortement souhaitable de le faire puisque cela s'inscrit dans le réseau de libre circulation de l'information.

Comme nous l'avons déjà souligné, l'expéditeur commercial a tout intérêt à s'assurer, dans la mesure du possible, que les personnes dont les noms figurent sur la liste d'envoi sont bien disposées à l'égard de l'envoi, que les listes ne renferment que les renseignements qui amélioreront la rentabilité de cet envoi, qui sont à jour et seront utilisés judicieusement.

Dans une étude commanditée par le Conseil de l'Europe, John Braun faisait l'observation suivante:

(traduction non officielle)

Si on accepte que l'utilisation du courrier est à la portée de tous (qu'il s'agisse de listes ou non) et que ce qui importe est la teneur du document posté et non pas le fait de le poster, ce qu'il importe alors de déterminer, c'est la question du préjudice. L'envoi postal renferme-t-il quelque chose qui va à l'encontre d'échanges commerciaux équitables, de l'honnêteté, de la moralité, du bon goût ou d'un des nombreux autres critères éventuels? Si le répondant est trompé ou susceptible d'être trompé ou fraudé ou indigné par la nature de la communication, il y a alors matière à intervention de la part de l'instance pertinente.

Dans la plupart des administrations, ces questions sont déjà visées par loi ou règlement. Ce qui n'est pas toujours visé et qui, d'après de plus en plus d'observateurs, ne devrait pas l'être, ce sont l'inscription, la teneur ou l'utilisation des listes de commercialisation directe par courrier.

Les raisons invoquées sont généralement le coût et le caractère peu applicable de ces mesures..

La raison la plus profonde et la plus éloquente est bien entendu que le processus d'auto-réglementation est de toute façon dans le meilleur intérêt des usagers, de la société et des destinataires.

Cela ne signifie pas qu'il n'y a pas d'abus ni de faiblesses ni de torts lorsqu'on utilise l'auto-réglementation. Il y en a, c'est certain; mais on peut constater que ces faiblesses sont bien moins importantes que celles qu'entraînent et peuvent entraîner des systèmes réglementés par voie législative.

Par exemple, pensez à l'anomalie d'une administration où il serait illégal de publier le sexe ou encore l'affiliation politique de membres sur une liste de noms et d'adresses des commettants d'une assemblée législative. Cette sorte de chose est l'un des risques d'une réglementation sur la vie privée dont le libellé serait trop strict.

Moins exagéré peut-être, mais tout aussi absurde, serait le cas où on exigerait des clubs d'enregistrer leurs listes de membres et de soumettre ensuite l'information que renferment ces listes à l'approbation de leurs membres. Cette précaution réglementaire empêcherait que la liste puisse être louée ou vendue à une entreprise commerciale qui pourrait légitimement vouloir envoyer de la documentation aux gens inscrits sur cette liste.

L'Organisation de coopération et de développement économiques a rendu publiques des directives régissant la protection de la vie privée dans la mesure où cela touche les listes de distribution, et ces directives ont été largement suivies. Les associations canadiennes et américaines de commercialisation directe par courrier et les groupes de mise en marché dans les pays européens, britanniques et scandinaves ont tous adopté des codes d'éthique et il vaut la peine de souligner que ces mesures ont été prises dans des pays où il existe des lois pertinentes aussi bien que dans des pays où il n'y en a pas.

Essentiellement, tous ces codes respectent les concepts et principes que renferme le code du Reader's Digest:

1. Les données personnelles recueillies et emmagasinées se limitent à celles qui ont trait à la rentabilité de la commercialisation, du traitement des commandes, de la prestation des services, de la facturation et de la perception des paiements en échange des produits et services de la société, et elles ne sont utilisées qu'à ces fins.
2. Les dossiers de données personnelles sont fréquemment mis à jour grâce à de nouveaux renseignements afin de s'assurer qu'ils sont précis, exhaustifs et d'actualité.
3. Reader's Digest répond promptement aux demandes écrites présentées par des clients ou d'autres personnes (ou leurs représentants juridiques reconnus) afin d'obtenir le résumé de leurs données personnelles contenues dans nos dossiers. Les données personnelles inexactes, dépassées ou incomplètes sont alors corrigées.

4. Sauf dans les cas de recouvrement de dettes au nom de Reader's Digest ou lorsque la loi l'exige, les données personnelles ne sont pas communiquées à des tierces parties.
5. Des mesures de sécurité strictes sont maintenues afin d'éviter l'accessibilité, la destruction, l'utilisation, la modification ou la divulgation non autorisées de données personnelles relatives aux clients de Reader's Digest.
6. La société Reader's Digest appuie les efforts des associations industrielles auxquelles elle appartient et qui favorisent la divulgation des politiques régissant l'échange ou la location de listes ainsi que la possibilité d'une formule d'exclusion de noms par les sociétés qui utilisent ces pratiques.
7. La société Reader's Digest se conforme promptement à toutes les demandes exprimées par les personnes qui ne désirent pas recevoir ses envois publicitaires, en inscrivant la mention appropriée au dossier. Ces demandes peuvent être reçues directement ou par l'intermédiaire de tierces parties, comme des associations de l'industrie ou de consommateurs ou des organismes gouvernementaux.
8. Reader's Digest respecte la totalité des lois et règlements locaux relatifs à la protection des données et au respect de la vie privée.

D'ailleurs, Reader's Digest ne procède ni à la location ni à l'échange des noms et adresses de ses clients.

Les sociétés progressistes adoptent de plus en plus des codes volontaires sérieux et bien formulés qui, s'ils renferment des éléments semblables à ceux exposés dans le document d'étude distribué à cette réunion, rendraient inutile toute loi autre qu'une loi bien générale.

En fonction de ces critères, la Commission de réforme du droit de l'Australie a, dans ses recommandations, établi un juste équilibre.

Avant de conclure cet exposé, il vaut peut-être la peine de répéter les éléments essentiels d'un code valable applicable à la gestion des listes:

- o les données personnelles doivent être recueillies et traitées équitablement et licitement;
- o les renseignements personnels doivent être conservés à une ou des fins précises et légitimes;

- o les données personnelles ne doivent pas être utilisées ou divulguées d'une façon incompatible avec ces fins;
- o les renseignements personnels doivent être appropriés, pertinents et non exagérés par rapport aux objectifs précisés;
- o les renseignements personnels doivent être précis et, si nécessaire, maintenus à jour;
- o les renseignements personnels ne doivent être rattachés à des noms précis que pour la période nécessaire aux fins précisées;
- o la personne visée par les données doit avoir accès aux renseignements qui sont conservés sur son compte et avoir le droit de les faire corriger ou supprimer lorsque les dispositions juridiques qui protègent les données personnelles n'ont pas été respectées;
- o il importe de prendre les mesures de sécurité appropriées contre l'accès, la modification ou la diffusion non autorisés, les pertes accidentelles et la destruction accidentelle ou non autorisée des données.

C'est l'auto-réglementation qui a poussé la Commission de réforme du droit de l'Australie à conclure ce qui suit:

(traduction non officielle)

Les avantages commerciaux que tirent les expéditeurs directs de l'adoption de ces méthodes (que j'ai déjà décrites), en particulier la réduction des coûts d'expédition, l'accroissement des bénéfices et de meilleures dispositions de la part du client, poussent les membres à vouloir maintenir ces formules. Cela facilite les avantages commerciaux du système d'expédition directe, notamment l'augmentation des ventes de produits et de services et l'élargissement des offres d'emploi, tout en réduisant le nombre des personnes qui reçoivent des envois importuns...

DOCUMENT: 870-123/009

CA1

I4

C52

INTERPROVINCIAL CONFERENCE ON PRIVACY:
INITIATIVES FOR 1984 (SYMPOSIUM)

The Delicate Balance: Reconciling Privacy Protection
with the Freedom of Information Principle

John D. McCamus
Dean
Osgoode Hall Law School
York University



Toronto, Ontario
May 23-24, 1984

THE DELICATE BALANCE: RECONCILING PRIVACY PROTECTION
WITH THE FREEDOM OF INFORMATION PRINCIPLE

by John D. McCamus *

A. Introduction

The underlying philosophy of the freedom of information concept is that, generally speaking, every citizen should have the right to obtain access to government records. The rationale offered for this most frequently is that the right of access will heighten the accountability of government and its agencies to the electorate, will enable interested citizens to contribute more effectively to debate on important questions of public policy and will conduce to fairness in administrative decision processes affecting individuals.

The philosophy underlying privacy protection, on the other hand, is in part at least that individuals should, generally speaking, have some control over the use made by others, especially government agencies, of information concerning themselves. Thus, it is often said that, again generally speaking, personal information acquired for one purpose should not be used for another purpose without the consent of the individual to whom the information pertains. This principle is thought to be an unworkable one in practical terms and thus is hedged by various exceptions in the usual forms of privacy protection legislation. Nonetheless, the principle represents the statement of an ideal from which the exceptions are taken.

When one focusses attention on government records containing personal information concerning identifiable individuals, it is perfectly obvious that these two philosophies and legislation based upon them are capable of generating an intense conflict. At the risk of belabouring the obvious, let us consider a few illustrations of the problem:

1. A journalist seeks access to government records that will reveal the salaries of the chief executive officers of all Crown corporations.
2. A researcher doing a study of military justice seeks access to records of decisions in all disciplinary matters.
3. A journalist who believes that a particular agency has been lax in dealing with a particular problem, seeks access to records which reveal the actions taken by responsible officials.
4. A convicted offender, released from prison under supervision, commits an offence of violence. A journalist seeks access to letters written in support of the prisoner's release.
5. A journalist seeks access to government records which he believes will reveal that a public servant has engaged in improper financial dealings.

One could easily multiply examples of this kind. In each case, the individual seeking access wishes to scrutinise some aspect of the conduct of public business. In some cases, this will involve disclosure of information pertaining to public officials. In others it will involve disclosure of information concerning ordinary citizens. In each instance, the subject of the information can plausibly raise a privacy protection concern. One man's freedom of information is another man's invasion of privacy.

The conflicts thrown up by these tensions between the freedom of information and privacy protection principles give rise to essentially three policy problems for those who are engaged in designing legislated freedom of information and privacy protection schemes. First, there arises the problem of institutional design. In what institutional form should conflicts of this kind be resolved? In the courts? In the legislature? In the bureaucracy? Second, wherever these problems are to be addressed, what guidance can be given to those saddled with the resolution of such conflicts? This is a question of substantive policy. How, if at all, can these two conflicting values be reconciled? In this paper, I will attempt to address these two questions and will do so against the background of a comparative analysis of Canadian and American freedom of information and privacy protection statutes and, the proposals of the Ontario Commission on Freedom of Information and Individual Privacy, set forth in the Commission's 1980 Report, *Public Government for Public People*.

A third range of problems, essentially technical in nature, will not be addressed here. These problems arise from the potential for conflict in the operation of general freedom of information laws and the rights conferred by privacy protection laws on data subjects to obtain access to information concerning themselves. It is no easy task to design access rights within these two different contexts which will co-exist harmoniously, and this has proven to be a continuing problem in the American federal experience. Suffice it

to say that in the Canadian context, these problems appear to have been for the most part resolved in the drafting of the Access to Information Act and the Privacy Act, as enacted in June of 1982.

B. The Institutional Design Problem: The Locus of Conflict Resolution

Turning to the first problem, then, given that conflict between the competing values of access to information and personal privacy appears inevitable, where should the power to provide an authoritative resolution of these conflicts reside? The answer provided by the American federal legislation is, as with so many other points of difficulty in both the freedom of information and privacy protection schemes, that the ultimate recourse is to be taken to the courts through judicial review of agency decisions to deny access. The U.S. Freedom of Information Act¹ requires that federal government agencies make their records available to "any person" unless the records fall within one of nine exceptions to this general rule. The exception of relevance to the present discussion is that agencies may refuse to disclose "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy".² An individual who is denied access to government record on the basis of the agency's conclusion that disclosure would be an unwarranted invasion of privacy, may challenge the agency's decision in the federal courts. The court will, in turn, reach its own conclusion as to whether or not the record is exempt from disclosure and, if satisfied that the public interest in access outweighs the individual data subject's interest in privacy, will

order disclosure of the doctrine in question.

The U.S. Privacy Act³ is drafted so as to function consistently with the access scheme. Thus, although the Act generally prohibits disclosure of personal data without the consent of the data subject, there are some exceptions to this general rule and one of them permits disclosures under the Freedom of Information Act. Thus, the Freedom of Information Act confers a right of access upon the requestor, the content of which is subject to judicial determination, and the Privacy Act confers a right of non-disclosure on the data subject, the content of which can again be tested in the courts. To be sure, for the litigation-averse public servant, a premium is placed on sound judgment when confronted with a request for access to a record containing personal information, the agency confronts the twin possibilities that if it denies access it may be sued under the Freedom of Information Act whereas if it grants access, it may be sued under the Privacy Act. Nonetheless, the American scheme does provide an independent source of authoritative advice on the resolution of the tension between access and privacy values. It is not at all surprising that a sophisticated jurisprudence on this question is emerging in the American case law.

Under the Canadian federal legislation, by way of contrast, reconciliation of the access and privacy values is left simply to the discretion of public officials. Thus, although the Access to Information Act⁴ confers a broad right of access to government records, it exempts from this right access to records containing "personal

information", this latter concept being very broadly defined indeed in the statute.⁵ This definition is itself subject to certain limited exceptions with the result that a very narrowly-conceived right of access to records containing personal information is contained in the Access to Information Act. As a general rule, however, access to such records is prohibited by the statute,⁶ though this prohibition is, in turn, made subject to whatever disclosures are permitted under Section 8 of the Privacy Act. The latter provision is the section of the Privacy Act which purports to control disclosure of personal information. Although it begins by stipulating that personal information shall not be disclosed without the consent of the individual data subject, it goes on to confer a series of discretionary powers on agencies to disclose information to a variety of individuals for a variety of purposes and concludes, in sub-section (m), that an agency has a discretion to disclose:

...for any purpose where, in the opinion of the head of the institution,

- (i) the public interest in disclosure clearly outweighs any invasion of privacy that could result from the disclosure, or
- (ii) disclosure would clearly benefit the individual to whom the information relates

The language of sub-paragraph (i) evinces a strong bias in favour of privacy protection, in contrast to the American provision which evinces strong support for the access principle, but this is a point to which we shall return in the next section of this paper. The important point for present purposes is that, as far as personal

information is concerned, essentially no right of access is conferred upon individuals seeking access and no right to control disclosure is conferred upon those who wish to prevent it. In sharp contrast to the American scheme, then, the Canadian statute confides this entire question to the discretion of agency officials.

In short, the Canadian scheme addresses the problem of resolving the conflict between access and privacy by simply surpressing it into a level of administrative discretion and withholding either rights of access or rights to prevent improper disclosure.

In adopting this approach, the Canadian scheme has, in my view, both substantially undermined the access rights conferred by the Access to Information Act and significantly depreciated the level of privacy protection afforded by the Privacy Act. As far as the access right is concerned, it should be emphasised that a very substantial percentage of government records must contain information pertaining to identifiable individuals which would bring it within the sweep of the far-reaching definition of personal information contained in these statutes. To confer a broad discretion to withhold or disclose such information on the federal bureaucracy itself is to simply ignore the basic premise of freedom of information legislation, i.e. that it is desirable to confer a right of access on the public at large. Public officials are placed in a position of conflict of interest when asked to disclose information which might facilitate effective scrutiny of their performance. The enactment of a freedom of information statute represents an acknowledgement of this plain fact and the adoption of a remedy which

places the decision to disclose the document effectively beyond the powers of the officials concerned. If it is the point of the federal Canadian scheme to sacrifice freedom of information in order to effect a high level of privacy detection, then it must also be said that the federal bureaucracy is not the most suitable instrument for the achievement of this objective. Again, public officials when confronted with requests for government records, are placed in a conflict of interest position. It may well be in the interests of a particular department to disclose information and demonstrate that it has conducted public affairs in a perfectly sound and responsible fashion, notwithstanding the substantial invasion of the privacy of identifiable individuals which may result from disclosure.

A leading American decision under the Freedom of Information Act illustrates the problem. In Sonderegger v. United States Department of the Interior,⁷ certain journalists sought access to claim files arising in the context of special federal assistance programmes to the victims of a flood which had devastated a town in Idaho. The journalists obviously wished to detect misfeasance in the handling of such claims and the federal agency involved was quite willing to permit full disclosure. The flood victims, on the other hand, felt that disclosure would not only substantially invade their privacy, inasmuch as each claim represented essentially the net worth of the individual in question, but would prove to be very stressful for the community which was enduring quite sufficient stress in attempting to re-establish itself after this disaster. Expert evidence was provided

by a psychologist who was working with the local committee, confirming this prognostication. The federal court decided that the public interest in disclosure was significantly outweighed by the resulting invasion of the privacy of the plaintiff townspeople and, thus, overruled the decision of the agency to permit disclosure. One can understand that public officials are anxious to dispel unfair allegations of wrongdoing. My point simply is that there will be contexts in which the question of disclosure cannot be approached in a completely disinterested fashion.

A substantial problem with the Canadian scheme, then, is that it establishes a far-reaching domain of discretionary power which, at one and the same time, creates the risk that access to records will be denied in order to preclude appropriate scrutiny of public affairs on the pretext that disclosure will unfairly invade the privacy of data subjects and, on the other hand, the risk that public officials concerned to clear their good names will be tempted to do so, notwithstanding the fact that disclosure will effect a substantial invasion of the personal privacy of individuals.

A further problem with the Canadian scheme is that it conduces to a wilderness of inconsistent decision-making from one department and governmental unit to the next. One finds little or no guidance in the statute itself as to how the discretion to disclose should be exercised. More surprisingly, perhaps, neither does one find assistance in the Treasury Board's Interim Policy Guide which sets forth extensive guidance for public officials on the proper interpretation and implementation of the Access to Information Act and the Privacy Act.

A more sympathetic view of the Canadian scheme would be to suggest that the legislation in its current form will provide an opportunity for the Information Commissioner and the Privacy Commissioner to investigate matters of this kind and assist the bureaucracy in developing helpful guidelines resolving conflicts of this kind. It is difficult to discern, however, that either Commissioner will have a substantial role in dealing with this issue. As far as the Information Commissioner is concerned, if the information in question clearly falls within the definition of personal information, and surely this will often be so, there does not appear to be much for her to say, other than that the record in question is, indeed, exempt from the access scheme. As far as the Privacy Commissioner is concerned, provided that the public official in question has, in good faith, weighed the public interest in disclosure against the privacy value, it is again difficult to see that much remains to be said by the Commissioner. It may well be, however, that given the importance of this question and the absence of any other source of guidance, either or both Commissioners will see fit to comment either on the inadequacies of the current legislative scheme or on the deficient exercise of the discretion which is unquestionably conferred upon public officials by it.

Two further explanations may be offered for the Canadian reluctance to extend judicial review into the area of personal records. First, it may be felt that this is an attempt to avoid burdening data subjects with either the cost or the inconvenience of participation in judicial review. Second, it may be thought that so important a

question as this ought not to be simply remitted to the courts.

With respect to the first point, a preferable solution would have been to endow the Privacy Commissioner with the power to clear the cost of litigation of this kind on behalf of the data subject. One of the great innovations of the Access to Information Act was to confer a power of this kind on the Information Commissioner in the context of access requests. Where the Information Commissioner believes that the information should be made available over the objection of the governmental institution in question, the Commissioner is entitled to carry to litigation on behalf of the requester and thus provide an authoritative resolution of the dispute which is cost-free to the requester. The Privacy Commissioner could have been similarly empowered to provide cost-free litigious protection to the data subject.

With respect to the appropriateness of the courts as the instrumentality for resolving these conflicts, it would appear that the only structural alternative to the bureaucracy itself would be the Legislature. Indeed, many statutes which establish administrative mechanisms requiring the collection of personal data do explicitly provide for the protection of the data and, while the notion of resort to the Legislature has an obvious democratic appeal in this context, two reservations about the capacity of the Legislature to deal effectively with these issues must be registered. First, a legislature dominated by a majority party is easily seen to be subject to a version of the same conflict of interest that plagues the Executive Branch. The Access to Information Act notwithstanding,

Canada is not likely to be vigorous in pursuit of a policy of drafting legislation so as to ensure effective scrutiny of its own conduct of public affairs. Secondly, it should be noted that many legislative provisions of this kind are currently to be found in the statute book and, consistently with the hypothesis just stated, they typically provide that there is to be no access whatsoever to the data in question. The concern that such provisions may conduce to too much secrecy is manifested in Section 24 of the Access to Information Act, which requires that all such provisions be reviewed by a Parliamentary Committee within three years of the enactment of the Access to Information Act. Accepting, as I do, that provisions of this kind relating to personal data were often enacted for the true motive of privacy protection, they are typically drafted without any evidence of sensitivity to the desirability of permitting some forms of access to even reasonably sensitive data. Thus, as Professor Flaherty demonstrated in a paper prepared for the Ontario Commission, much useful medical research has been thwarted by the existence of provisions of this kind.

Leaving these reservations aside, however, it nonetheless is true that one possible response to the concern that the courts should not be given too much discretion in matters of this kind would be to specifically enact access and disclosure schemes to deal with specific information contexts. Whether the reconciliation of privacy and access principles is to be located in the Legislature or the Courts or the bureaucracy, or perhaps all three, the difficult question that remains, and to which we now turn, is how one should

approach the task of effecting that reconciliation in analytical terms.

C. The Substantive Problem: Achieving an Appropriate Balance

Again, the American and Canadian models provide interesting points of contrast. As has been indicated, the American statute provides a right of access unless disclosure of personal data would constitute a "clearly unwarranted invasion of privacy". The Canadian statute, on the other hand, provides for essentially no right of access, but for the right to obtain documents containing information in three categories:

- 1) Certain basic information concerning the contracts of employment of public servants and their opinions or views given in the course of employment;
- 2) Similar information concerning individuals performing services for a government institution under contract; and
- 3) Information "relating to any discretionary benefit of a financial nature, including the granting of a licence or permit"⁸

Presumably, the draftsmen of the Canadian statute thought that a more precise provision of this kind had some advantages over the vague standard of the American "clearly unwarranted invasion of privacy" test. Nonetheless, the difficulties created by a refusal to embrace a balancing test of some kind are manifest in this provision. As an access right, the Canadian provision leaves much to be desired. The illustrations with which I began this paper were carefully chosen with this point in mind. They are all situations in which, in my view,

a strong claim for access can be made and they are all situations in which access would be granted under the American scheme, notwithstanding the fact that all involve disclosure of personal information. They are also all situations in which no access would be given under the Canadian statute.

From the privacy protection point of view, the Canadian provision is also flawed. Although one understands the obvious rationale for requiring disclosure of information relating to discretionary benefits such as licences, it should be noted that most welfare schemes of one sort or another contain modest discretionary features. Thus, whether we speak of unemployment insurance benefits or widows' benefits under veterans' administration legislation, or the various forms of assistance we render to those suffering from mental or physical disabilities, some financial benefits typically remain within a discretionary category. There appears to be no merit whatsoever in conferring, as the Canadian statute does, a right of access to personal data pertaining to discretionary benefits of this particular kind.

A strong case can be made, then, for the need for a balancing test of some kind. Indeed, this is accepted in the Canadian statute to the extent that apart from this limited right of access to personal data conferred in the Access to Information Act, all other disclosures are to be made, though purely as a matter of administrative discretion, on the basis of a balancing test. The question that remains to be considered is how should this balancing test ideally be designed? Before offering some suggestions to this end, two

preliminary points can usefully be addressed.

First, it should be noted that to some extent the conflict between freedom of information and privacy protection can be resolved by deleting the names of identifiable individuals before releasing the requested documents. Anonymous data of this kind will often meet the needs of the requester and retard, if not completely eliminate, the risk of privacy invasion. As the leading U.S. case of U.S. Department of the Air Force v. Rose⁹ indicates, however, even where some risk of identification or privacy invasion remains, deletion of names may make the task of balancing the public interest in access against the risk of privacy invasion an easier one. In Rose, legal researchers engaged in a study of military discipline sought access to records relating to Air Force disciplinary proceedings. They conceded that access to records with names deleted would be sufficient for their purpose but it was objected by the defendant that even with names deleted, it would be possible in many instances for individuals who were familiar with the incidents in question to identify the person disciplined. The Federal Court held that although this risk was present, it was outweighed in the present case by the public interest in the ability of outsiders to scrutinise this area of government activity.

In any case where the deletion of names or other identifying detail has the effect of preventing the identification of individuals, the requester should be able to ? principle of segregability, i.e. the principle embraced by both the American and Canadian access statutes that the government must disclose any reasonably segregable

portion of a requested document that is not covered by one of the exemptions. The lesson from the Rose case, however, is that even where the elimination of identifiability can not be achieved in this way, one may nonetheless reduce the risk of privacy invasion to the point where it is outweighed by the public interest in access

A second point which has surfaced in the American case law applying the "clearly unwarranted invasion of privacy" test is whether the specific use of the personal data proposed by the requester is to be relied upon as the basis for testing the public interest in disclosure. Thus, where the requester has some highly beneficial medical or other research in mind, it is that the potential benefit of such research must be weighed against the invasion of privacy or, inasmuch as disclosure is likely to mean that the personal data can have a wider circulation in the public domain, should the particular use of the requester be ignored? In the U.S. experience and literature, discussion of this issue has been provoked by the decision in Getman v. NLRB¹⁰, a case in which certain law professors specializing in labour relations were allowed access to the names of union members who had voted for certification of a trade union in order to carry out research on certain policies of the U.S. National Labour Relations Board relating to the certification process. The court in Getman awarded access to the requesters specifically for the purpose of this project, and on the faith of an undertaking by them that they would not disclose the names of the individuals to anyone else. It is evident that the disclosure of these names to the employer at an early stage in the

process or to the public at large would clearly amount to an unwarranted invasion of personal privacy. In Getman, then, the Court was prepared to grant limited access to the particular requester, even though access to the public at large would be inappropriate.

The debate stimulated by Getman has been rather intense. Some have objected to the decision on the grounds that inasmuch as the Freedom of Information Act provides access to "any person" the particular requesters "need to know" ought to be considered irrelevant. Others have had a policy justification for this reading of the statute which, to my mind at least, is compelling. If one does embrace a "need to know" concept in some of this case law, it is likely to spread its influence throughout the case law dealing with the conflict between freedom of information and privacy protection and very substantially undermine the value of the access right. Moreover, it seems impractical to contemplate a general practice of trying to restrain further disclosures of information released to requesters under the Freedom of Information Act. A far better solution, it seems to me, and one that was in fact proposed in the report of the Ontario Commission, was to treat the problem of access for research purposes as a separate problem and to devise a mechanism for providing access to personal data for the research community.¹¹

Turning then to the central question, how is one to strike a balance between freedom of information and privacy protection, the question essentially is whether one can do any more by way of

providing guidance to decision-makers than offering the general instruction provided, albeit in significantly different terms, by both the American and Canadian statutes that the decision-maker should carefully weigh the public interest in disclosure against the personal interest in privacy protection. My own view is that one can substantially improve on this approach by attempting to articulate a variety of more explicit factors that should be taken into account by someone undertaking the task of reconciling these two interests. The following propositions derive, in the main, from discussion set forth in the Ontario Report to the same general effect and from a recent re-reading of the American case law applying the "clearly unwarranted invasion of privacy" test.

I would suggest that the following factors should be considered pertinent in attempting to balance these conflicting interests:

- a) Is access to the information necessary to enable an individual to accomplish any of the objectives underlying freedom of information legislation, i.e. effective scrutiny of the activity of government institutions, effective participation in discussion concerning public affairs and increased fairness in administrative decision-making affecting individuals.

As I have already indicated, it may be asking too much of human nature to allow public officials themselves to determine whether a particular request is well suited to accomplish these objectives. These questions are not particularly difficult ones, however, and could I think be answered fairly confidently by third parties in most instances.

- b) Is access to the information in question likely to make a positive contribution to the promotion of public health or safety?

In addition to the generally-accepted political rationales articulated in point a), the granting of access to information with this objective in view appears to be accepted as a desirable spinoff of freedom of information legislation and provides a particularly intense interest in access.

- c) Will access to the information in question promote an informed choice in the purchase of goods and services?

Again, this appears to be an incidental spinoff of freedom of information schemes.

Both item b) and item c) find some philosophical support in Section 20 of the Canadian Access to Information Act which explicitly provides for access to the results of product and environmental testing and, more generally, confers upon government institutions a discretion to disclose commercial information if the public interest in public health, public safety or protection of the environment outweighs the harm that might result to the commercial party to whom the information pertains.

- d) Will the granting of access have the effect of benefitting the individual who is the subject of the information disclosed?

There may well be situations where the individual seeking access has only in mind the conferral of some benefit on the data subject and the case for disclosure in such circumstances is obviously compelling.

This consideration is explicitly set forth in Section 8(m) of the Privacy Act as a basis for exercising the discretion to disclose. Is the information of a kind which is normally disclosed in other contexts?

Illustration 4 at the beginning of this paper asked whether letters written in support of the release of a prisoner should be available to the public. These were the facts of a decision under the American Act, Philadelphia Newspapers Inc. v. U.S. Department of Justice¹² in which the court reasoned that inasmuch as such individuals are acting, in a sense, as character witnesses for the convicted person, something they would normally be required to do in a public hearing, the letter should be made available. Here, as elsewhere in legal analysis, a fruitful analogy is an important source of guidance.

A number of factors may be taken to weigh in the balance against disclosure:

- e) Will access to the information frustrate the objectives of the statutory scheme under which the information was originally collected?

There may well be situations, for example, where conciliation procedures are mandated by a statute, where a disclosure of records will render the governmental institution in question effectively unable to carry out its assigned statutory task. Surely this would weigh heavily against disclosure.

- f) Is the personal information of an especially sensitive kind?

It is possible to identify types of information such as medical information or information relating to eligibility for social service

or welfare benefits, the disclosure of which would be seen by the average data subject as an especially grievous invasion of privacy.

- g) Is the information unlikely to be accurate or reliable?

The probability that personal data will be accurate may vary quite considerably on the circumstances under which it is gathered or submitted, and the safeguards established or verification procedures adopted by the government institution in question. Surely the likelihood of circulating inaccurate information should weigh against a decision to disclose.

- h) Is there some prospect that the data subject will suffer substantial harm, pecuniary or otherwise, as a result of the disclosure?

Some invasions of privacy may serve not only to embarrass or otherwise diminish the sense of privacy of the individual data subject, but also cause substantial harm of one sort or another. This, again, should weigh against disclosure.

- i) Was the information submitted on the basis of an expectation, tacit or otherwise, that it would be treated in a confidential fashion?

An American court has suggested that, although an undertaking of confidentiality should weigh heavily against disclosure, it should merely be a factor taken into account in determining whether or not to make the information available.¹³ Presumably such undertakings would normally be adhered to but perhaps not, for example, where the individual who initially supplied the information did not rely on

the undertaking in any meaningful sense or could have been required by law submit the information in question.

No doubt intimate experience with the functioning of freedom of information and privacy protection schemes will enable one to offer further principles of this kind.

The Ontario Commission recommended a rather elaborate statutory provision¹⁴ in which a number of the foregoing propositions were stated as presumptions to be employed in the application of the balancing test and, I confess, I remain convinced that this is an attractive solution to the problem presented in this paper. At the very least, however, it seems to me that the articulation of principles of this kind should be of assistance to those charged with the task of applying the more vague standards set forth in the American and Canadian legislation.

Privacy is an important but surely not an absolute value, and one which must compete with other values such as that so widely accepted today of the public interest in access to government information. When confronted with the difficulty of reconciling these conflicting values, it appears that the draftsmen of the Canadian scheme shied away from the task. It is hoped that the foregoing analysis will be of some assistance to those who must attempt to strike an appropriate balance between access and privacy in exercising their discretionary powers under Section 8(m) of the Privacy Act.

Footnotes

* Dean, Osgoode Hall Law School of York University. Copyright reserved.

1. 5 U.S.C. Section 552.
2. Id, (b) 6.
3. 5 U.S.C. Section 552a.
4. Canada, Parliament, First Session, 32nd Parliament, 1980, House of Commons, Bill C-43 (An Act to Enact the Access to Information Act and the Privacy Act, to amend the Federal Court Act and the Canada Evidence Act, and to amend certain other Acts in consequence thereof) as passed by the House of Commons, June 28, 1982, hereafter the "Access to Information Act" or the "Privacy Act".
5. Privacy Act, Section 3.
6. Access to Information Act, Section 19(2).
7. 424 F. Supp. (1976).
8. Privacy Act, Section 3, (j) to (l) of the definition of "personal information".
9. 425 U.S. 352 (1976).
10. 450 F 2d 670 (DC Cir 1971).
11. Ontario Commission on Freedom of Information and Individual Privacy, Final Report: Public Government for Private People (1980), Vol. 2, 332-334.
12. 405 F. Supp. 8 (ED Pa 1975).
13. Robles v. EPA, 484 F 2d 843 (4th Cir 1973).
14. Supra, note 11 at pp. 335-338.

DOCUMENT: 870-123/009

CONFÉRENCE INTERPROVINCIALE SUR LA PROTECTION DES
RENSEIGNEMENTS PERSONNELS:
MESURES POUR 1984 (COLLOQUE)

Un équilibre fragile: comment concilier la protection des renseignements
personnels avec le principe de la liberté d'accès à l'information

John D. McCamus
Doyen
Osgoode Hall Law School
Université York



Toronto, Ontario

23-24 mai 1984

UN ÉQUILIBRE FRAGILE: COMMENT CONCILIER LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS AVEC LE PRINCIPE DE LA LIBERTÉ D'ACCÈS À L'INFORMATION

par John D. McCamus*

A. Introduction

Le principe directeur du concept de liberté d'accès à l'information est le suivant: tout citoyen devrait en principe avoir un droit d'accès aux dossiers du gouvernement. La justification la plus fréquemment avancée est que le droit d'accès rendra le gouvernement et ses organismes plus responsables face à l'électorat, permettra aux citoyens concernés de participer plus efficacement aux débats sur les questions publiques importantes et suscitera une plus grande équité dans les processus décisionnels administratifs concernant les individus.

Par ailleurs, le principe directeur de la protection des renseignements personnels est le suivant, à tout le moins en partie: les individus devraient en principe avoir un certain contrôle sur l'utilisation, par d'autres personnes et en particulier les organismes gouvernementaux, des renseignements qui les concernent. On entend donc souvent dire que, là encore sur un plan général, les renseignements personnels obtenus dans un but donné ne devraient pas être utilisés à d'autres fins sans le consentement de la personne concernée. Ce principe est difficile à mettre en pratique et il est donc assorti de diverses exceptions, qui prennent généralement la forme de lois sur la protection

des renseignements personnels; il représente néanmoins l'expression d'un idéal à partir duquel les exceptions sont prévues.

Lorsqu'on s'arrête aux dossiers gouvernementaux contenant des renseignements personnels au sujet de personnes identifiables, il devient parfaitement évident que ces deux principes et la législation qui en découle sont susceptibles de provoquer de sérieux litiges. Au risque de souligner des évidences, envisageons quelques illustrations du problème:

1. Un journaliste demande à consulter des dossiers du gouvernement qui révéleront les salaires des présidents directeurs généraux de toutes les sociétés de la Couronne.
2. Un chercheur faisant une étude sur la justice martiale désire consulter toutes les décisions rendues en matière disciplinaire.
3. Croyant qu'un organisme a fait preuve de négligence face à un problème donné, un journaliste, veut avoir accès aux documents révélant les mesures prises par les fonctionnaires responsables.
4. Un contrevenant condamné, mis en liberté sous surveillance, commet une infraction violente. Un journaliste demande à consulter les lettres écrites afin de justifier la mise en liberté du détenu.
5. Un journaliste demande à consulter des dossiers du gouvernement qui, selon lui, révéleront qu'un fonctionnaire a fait des transactions financières douteuses.

On pourrait facilement multiplier de tels exemples. Dans chaque cas, la personne qui demande l'accès aux renseignements désire examiner de plus près un aspect quelconque de la conduite des affaires publiques. Dans certains cas, cela implique la communication de renseignements au sujet de fonctionnaires; dans d'autres cas, cela entraîne la communication de renseignements concernant des citoyens ordinaires. Dans chaque cas toutefois, la personne visée par la demande peut s'inquiéter à juste titre de la confidentialité des renseignements qui la concernent: La liberté d'accès à l'information d'une personne s'arrête là où commence l'empiètement sur la vie privée d'autrui.

Les conflits suscités par cette opposition entre le principe de la liberté d'information et celui de la protection de la vie privée posent essentiellement trois problèmes de principe aux personnes chargées de concevoir les mécanismes législatifs assurant la liberté de l'information et la protection des renseignements personnels. Premièrement, surgit le problème du cadre institutionnel: quelle institution devrait statuer sur les conflits de ce genre? Les tribunaux? La législature? La bureaucratie? Deuxièmement, quelle que soit l'institution à qui l'on confie le soin de régler ces problèmes, quelles lignes directrices peut-on donner aux personnes qui en sont chargées? Il s'agit là d'une question de fond. Comment peut-on concilier ces deux valeurs contradictoires; est-il même possible de le faire? Dans ce document, j'essaierais de répondre à ces deux questions en faisant une analyse comparative des législations canadienne et américaine sur la liberté de l'information et la protection

des renseignements personnels, et en m'inspirant des propositions de la Commission on Freedom of Information and Individual Privacy de l'Ontario, énoncées dans le rapport de 1980 de la Commission, Public Government for Public People.

Il existe une troisième série de problèmes, essentiellement de nature technique, auxquels je ne m'attacherai pas ici. Ces problèmes résultent du conflit potentiel d'application entre les lois générales sur la liberté de l'information et les lois sur la protection des renseignements personnels, qui donnent aux personnes visées un droit d'accès aux renseignements qui les concernent. L'élaboration de droits d'accès pouvant co-exister harmonieusement dans ces deux cadres contradictoires n'est pas tâche facile; elle s'est révélée un problème persistant au niveau fédéral aux États-Unis. Disons simplement que ces problèmes semblent avoir été pour la plupart résolus au Canada par la Loi sur l'accès à l'information et la Loi sur la protection des renseignements personnels, édictées au mois de juin 1982.

B. Le problème du choix institutionnel: la compétence sur le règlement
des litiges

Abordons le premier problème: étant que le conflit entre les valeurs contradictoires de l'accès à l'information et de la protection des renseignements personnels semble inévitable, à quelle entité devrait-on donner autorité pour statuer sur ces litiges? La législation fédérale des États-Unis prévoit que, tout comme pour les nombreux autres sujets contentieux dans les mécanismes de liberté de l'information et de

protection des renseignements personnels, l'on doit s'adresser aux tribunaux pour faire réviser les décisions des organismes qui refusent de communiquer des renseignements. La Freedom of Information Act¹ des États-Unis oblige les organismes gouvernementaux à mettre leurs dossiers à la disposition de "toute personne", à moins qu'ils n'entrent dans l'une des neuf exceptions à cette règle générale. L'exception pertinente à notre propos prévoit que les organismes peuvent refuser de communiquer "des dossiers personnels et médicaux, et des dossiers semblables, dont la communication constituerait une violation injustifiée de la vie privée".² Une personne qui se voit refuser l'accès à des dossiers gouvernementaux pour ce motif peut contester la décision de l'organisme devant les tribunaux fédéraux. Le tribunal déterminera lui-même si l'exception à l'obligation de divulgation, s'applique à ces dossiers et, s'il est convaincu que des raisons d'intérêt public justifient un empiètement sur le droit à la vie privée de la personne concernée, ordonnera que ces renseignements soient communiqués.

La Privacy Act³ des États-Unis est conçue en vue d'une application compatible avec le mécanisme d'accès à l'information. Par conséquent, bien que la loi interdise généralement la communication des données personnelles sans le consentement de la personne concernée, il existe certaines exceptions à cette règle générale, dont l'une permet les communications aux termes de la Freedom of Information Act. Par conséquent, la Freedom of Information Act donne aux demandeurs un droit d'accès dont l'étendue est sujette à une décision judiciaire, et la Privacy Act donne à la personne

concernée un droit à la confidentialité des renseignements, dont la portée peut également être contestée devant les tribunaux. En ce qui concerne les fonctionnaires, qui n'éprouvent qu'aversion pour les litiges, on s'en remet à leur jugement éclairé lorsqu'une personne demande l'accès à un dossier contenant des renseignements personnels; dans un tel cas, l'organisme fait face à une double possibilité d'actions en justice, puisqu'il peut être poursuivi aux termes de la Freedom of Information Act s'il refuse de communiquer des renseignements, et aux termes de la Privacy Act s'il les communique. Le système américain prévoit néanmoins une autorité indépendante chargée de résoudre le conflit entre ces valeurs: accès à l'information et protection de la vie privée. Il n'est aucunement surprenant qu'une jurisprudence très élaborée sur cette question commence à prendre forme aux États-Unis.

Aux termes de la législation fédérale canadienne, par contre, on laisse simplement aux fonctionnaires le pouvoir discrétionnaire de concilier les valeurs de l'accès à l'information et de la protection des renseignements personnels. Par conséquent, bien que la Loi sur l'accès à l'information⁴ donne un large droit d'accès aux dossiers du gouvernement, ce droit ne s'applique pas aux dossiers contenant des "renseignements personnels", ce dernier concept étant défini extrêmement largement dans la loi.⁵ Cette définition est elle-même sujette à certaines exceptions limitées, de telle sorte que la Loi sur l'accès à l'information donne un droit d'accès très restreint aux dossiers contenant des renseignements personnels. En règle générale, toutefois, l'accès à ces documents est interdit par la loi,⁶ bien que cette interdiction soit elle-même assujettie aux obligations de communication prévues par l'article 8 de la Loi sur la

protection des renseignements personnels. Cette dernière disposition est l'article de la Loi sur la protection des renseignements personnels qui vise à contrôler la communication des renseignements personnels. Bien que le début de cet article stipule que les renseignements personnels ne peuvent être communiqués sans le consentement de l'individu qu'ils concernent, il confère par la suite une série de pouvoirs discrétionnaires aux organismes, leur permettant de communiquer des renseignements à divers individus et pour divers motifs; cet article conclut, au sous-alinéa (m) qu'un organisme a le pouvoir discrétionnaire de communiquer des renseignements personnels pour:

- "...communication à toute autre fin dans les cas où, de l'avis du responsable de l'institution,
- i) des raisons d'intérêt public justifieraient nettement une éventuelle violation de la vie privée,
 - ii) l'individu concerné en tirerait un avantage certain."

La formulation du sous-alinéa (i) révèle un parti pris très marqué en faveur de la protection des renseignements personnels, par comparaison à la disposition américaine qui favorise plutôt le principe de l'accès à l'information, mais c'est là un point sur lequel nous reviendrons dans la section suivante de ce document. L'élément important à souligner pour l'instant est que, en ce qui concerne ces renseignements personnels, la loi ne confère fondamentalement aucun droit aux individus qui veulent obtenir des informations, pas plus qu'elle ne donne un droit de contrôle sur la communication de renseignements à ceux qui veulent l'empêcher. La Loi

canadienne se démarque donc très nettement du système américain dans la mesure où elle laisse toute discrétion aux fonctionnaires de l'organisme.

En résumé, le système canadien remédie au problème du conflit entre l'accès à l'information et la protection de la vie privée en l'assujettissant à une décision administrative discrétionnaire, et en retirant à la fois le droit d'accès à l'information et le droit d'empêcher une communication inopportune.

À mon avis, l'approche retenue pour le système canadien restreint à la fois les droits d'accès conférés par la Loi sur l'accès à l'information et amoindrit de façon significative la protection de la vie privée prévue dans la Loi sur la protection des renseignements personnels. En ce qui concerne le droit d'accès à l'information, il faut souligner qu'une proportion très importante des documents gouvernementaux contient des renseignements concernant des individus identifiables, ce qui les ferait entrer dans la très large définition des "renseignements personnels" contenue dans ces lois. Le fait de donner à la bureaucratie fédérale un large pouvoir discrétionnaire de retenir ou de communiquer ces renseignements équivaut simplement à ignorer le postulat fondamental de la législation sur la liberté de l'information, c'est-à-dire qu'il est souhaitable de donner un droit d'accès au grand public. Les fonctionnaires se trouvent dans une situation de conflit d'intérêt, lorsqu'on leur demande des renseignements qui pourraient faciliter un examen approfondi de leur rendement. En adoptant une loi sur la liberté d'information, on constate simplement ce fait, et l'on adopte un recours qui ôte aux fonctionnaires

concernés le pouvoir de décider si le document doit être communiqué. Si le système canadien entend sacrifier la liberté de l'accès à l'information à une protection plus étroite des renseignements personnels, il faut alors également affirmer que la bureaucratie fédérale n'est pas le meilleur moyen pour atteindre cet objectif. Une fois de plus, les fonctionnaires sont en situation de conflit d'intérêt lorsqu'une personne demande à consulter des documents gouvernementaux. Il pourrait fort bien survenir des cas où un ministère donné aurait intérêt à communiquer des renseignements et à démontrer qu'il s'est occupé des affaires publiques d'une façon parfaitement légitime et responsable, malgré les violations substantielles de la vie privée d'individus identifiables qui pourraient résulter de cette communication.

Un arrêt de principe rendu aux termes de la Freedom of Information Act des États-Unis illustre ce problème. Dans l'affaire Sonderegger v. United States Department of the Interior,⁷ certains journalistes avaient demandé à consulter les dossiers des réclamations produites, dans le cadre d'un programme spécial d'aide fédérale, par les victimes d'une inondation qui avait dévasté une ville dans l'Idaho. Les journalistes désiraient de toute évidence relever les erreurs qui auraient pu se produire dans le traitement de ces plaintes, et l'organisme fédéral concerné était tout disposé à communiquer tous les renseignements voulus. Les victimes de l'inondation, par contre, estimaient que cette communication constituerait non seulement une violation grave leur vie privée, puisque le montant de chaque réclamation représentait essentiellement le patrimoine net de l'individu en question, mais qu'elle créerait également de graves tensions au sein de la

communauté qui essayait de se remettre du désastre, ce qui la perturbait déjà suffisamment. Ce pronostic fut confirmé par un psychologue qui travaillait avec le comité local, et qui fut appelé comme témoin-expert. La Cour fédérale a décidé que les considérations d'intérêt public en faveur de la communication ne pouvaient justifier la violation de la vie privée des demandeurs, et a donc renversé la décision de l'organisme permettant la communication des renseignements. On peut fort bien comprendre que des fonctionnaires soient très désireux de dissiper les accusations injustifiées de malversations portées contre eux; je veux simplement souligner qu'il existe des situations où cette question de communication ne peut être abordée de façon complètement désintéressée.

Le système canadien comporte donc une difficulté substantielle, car il confère des pouvoirs discrétionnaires très larges: Il se pourrait que des fonctionnaires refusent l'accès à des documents afin d'empêcher un examen approfondi et approprié des affaires publiques sous prétexte que cette communication entraînerait une violation de la vie privée des personnes concernées; d'autre part, il se peut que des fonctionnaires désireux de se laver de tout soupçon soient tentés de communiquer des renseignements, même au prix d'une violation substantielle de la vie privée d'individus.

Le système canadien comporte une autre difficulté, soit le manque d'uniformité prévisible dans les décisions rendues par les différents ministères et organismes gouvernementaux. La Loi ne donne que peu d'indications, voire aucune, sur la façon dont cette discrétion doit être

exercée. Et ce qui est peut-être plus surprenant, on ne trouve pas plus de lignes directrices dans le Guide provisoire du Conseil du Trésor, qui donne de nombreux renseignements aux fonctionnaires sur l'interprétation et l'application adéquates de la Loi sur l'accès à l'information et de la Loi sur la protection des renseignements personnels.

On pourrait voir le système canadien sous un jour plus positif et suggérer que la législation sous sa forme actuelle donnera au Commissaire à l'information et au Commissaire à la protection de la vie privée l'occasion de faire enquête sur les questions de ce genre, et d'aider la bureaucratie à élaborer des lignes directrices qui permettront de résoudre de tels conflits. Toutefois, il est difficile de prévoir si l'un ou l'autre des commissaires jouera un rôle important en cette matière. En ce qui concerne la Commissaire à l'information, si les renseignements en question entrent clairement dans la définition des renseignements personnels, ce qui sera certainement fréquemment le cas, il semble qu'elle n'aura pas un grand pouvoir d'intervention, sauf bien entendu pour déclarer que le document en question ne peut être communiqué. Par ailleurs, le Commissaire à la protection de la vie privée n'aura pas grand-chose à ajouter si le fonctionnaire en question a, de bonne foi, comparé l'intérêt public à la communication à la protection de la vie privée. Toutefois, il se pourrait bien qu'en raison de l'importance de cette question et de l'absence de toute autre ligne directrice, l'un ou l'autre des commissaires, ou les deux, jugent approprié d'exprimer leurs commentaires sur les lacunes du mécanisme législatif existant, ou sur l'exercice inapproprié de la discrétion que la législation confère indubitablement au fonctionnaire.

On peut avancer deux autres explications à la réticence canadienne à confier aux tribunaux le pouvoir de réviser les décisions prises à l'égard des documents personnels. Premièrement, il se peut qu'on ait voulu éviter aux personnes concernées par ces renseignements les frais ou les inconvénients du processus judiciaire. Deuxièmement, on a pu juger qu'il s'agissait d'une question si importante qu'on ne devrait tout simplement pas la confier aux tribunaux.

En ce qui a trait au premier point, il aurait été préférable de donner au Commissaire à la protection de la vie privée le pouvoir d'acquitter les frais des litiges de ce genre au nom de la personne visée par les renseignements. L'une des grandes innovations de la Loi sur l'accès à l'information a été de donner un tel pouvoir au Commissaire à l'information, dans le cadre des demandes d'accès à l'information. Lorsque le Commissaire à l'information estime que l'information devrait être communiquée malgré les objections de l'institution gouvernementale en question, il peut instituer des poursuites au nom du demandeur et provoquer ainsi le règlement du litige, sans qu'il en coûte quoi que ce soit au demandeur. Il aurait été possible de donner au Commissaire à la protection de la vie privée des pouvoirs semblables lui permettant d'intenter des poursuites au nom des personnes concernées, sans qu'il leur en coûte quoi que ce soit.

En ce qui concerne le bien-fondé du recours aux tribunaux pour résoudre ces litiges, il semblerait que la seule solution de rechange à la bureaucratie elle-même soit la législature. De fait, de nombreuses lois

établissant des mécanismes administratifs exigeant la collecte de données personnelles prévoient expressément que celles-ci doivent être protégées et, bien que l'idée de faire appel à la législature présente un attrait démocratique évident, deux réserves s'imposent sur l'aptitude de la législature à s'occuper efficacement de ces problèmes. Premièrement, une législature dominée par un parti majoritaire pourrait facilement sembler être dans une position de conflit d'intérêt semblable à celle du pouvoir exécutif. Malgré l'existence de la Loi sur l'accès à l'information, le Canada ne poursuivrait vraisemblablement pas de façon très active une politique visant l'adoption de lois permettant d'examiner sérieusement la façon dont il conduit les affaires publiques. Deuxièmement, il faut souligner que de nombreuses dispositions législatives de ce genre existent actuellement dans les lois et, conformément à l'hypothèse que nous venons d'énoncer, prévoient généralement qu'il est interdit d'avoir accès aux données en question. L'article 24 de la Loi sur l'accès à l'information, qui prévoit qu'un comité parlementaire doit examiner toutes les dispositions de ce genre dans les trois ans qui suivent l'entrée en vigueur de la loi, est révélateur des craintes qu'elles suscitent, c'est-à-dire une extension exagérée de la confidentialité). En admettant, comme je le fais, que les dispositions de ce genre relatives aux données personnelles ont souvent été adoptées dans le but premier de protéger la vie privée, on peut constater que leurs auteurs les ont généralement rédigées sans se demander s'il serait souhaitable de permettre un certain accès à des données, même relativement confidentielles. Par conséquent, comme l'a démontré le professeur Flaherty dans un document préparé pour la Commission de l'Ontario, de nombreuses recherches médicales utiles ont été entravées par l'existence de dispositions de ce genre.

Ces réserves mises à part, il reste néanmoins vrai qu'une des solutions possibles au refus de donner un trop grand pouvoir discrétionnaire aux tribunaux en cette matière consisterait à prévoir dans une loi des mesures spécifiques d'accès et de communication dans le cadre de contextes d'information particuliers. Que l'on confie à la législature, aux tribunaux, à la bureaucratie, ou peut-être même aux trois à la fois, le soin de concilier les principes de la protection des renseignements personnels et de l'accès à l'information, la question complexe qui subsiste, et que nous aborderons maintenant, est la suivante: comment formuler en termes analytiques les mesures permettant cette conciliation?

C. Le problème substantif: comment atteindre un équilibre satisfaisant?

Une fois de plus, il est intéressant de mettre en opposition les modèles canadien et américain. Comme nous l'avons mentionné, la loi américaine prévoit un droit d'accès à moins que la communication des données personnelles ne constitue une "violation clairement injustifiée de la vie privée". Par contre, la loi canadienne ne donne fondamentalement aucun droit d'accès, à l'exception du droit d'obtenir des documents contenant des renseignements appartenant à trois catégories:

- 1) Certains renseignements fondamentaux concernant les contrats d'emploi de fonctionnaires et les idées et opinions personnelles exprimées au cours de l'emploi;

- 2) Les renseignements semblables concernant des personnes exécutant un contrat de prestation de services pour une institution gouvernementale; et
- 3) Des renseignements sur "des avantages financiers facultatifs, notamment la délivrance d'un permis ou d'une licence accordés à un individu".⁸

Il y a tout lieu de penser que les rédacteurs de la loi canadienne estimaient qu'une disposition plus précise de ce genre présentait certains avantages par rapport à la norme vague de "la violation clairement injustifiée de la vie privée", prévue dans la loi américaine. Néanmoins, les difficultés entraînées par le refus d'adopter un critère comparatif quelconque sont manifestes dans cette disposition. Les droits d'accès conférés par la disposition de la loi canadienne laissent fort à désirer. J'ai soigneusement choisi les exemples donnés au début de ce document en songeant à cet argument. Il s'agit dans tous les cas de situations où, à mon avis, des motifs valables militent fortement en faveur de l'accès à l'information et où le système américain permettrait cet accès, malgré que ces situations impliquent toutes la communication de renseignements personnels. Par ailleurs, ce sont également toutes des situations où la loi canadienne ne permettrait pas l'accès à l'information.

La législation canadienne comporte également des lacunes en ce qui concerne la protection des renseignements personnels. Bien qu'il soit facile de comprendre la justification évidente de la confidentialité des renseignements concernant les avantages facultatifs, comme les licences, on

doit souligner que la plupart des mécanismes de bien-être présentent certains aspects discrétionnaires mineurs; ainsi, qu'il soit question des prestations d'assurance-chômage, des prestations accordées aux veuves aux termes de la législation sur les anciens combattants, ou des diverses formes d'aide aux personnes souffrant d'incapacité physique ou mentale, certains avantages financiers conservent généralement un caractère discrétionnaire. Il ne semble aucunement justifié de donner, comme le fait la loi canadienne, un droit d'accès aux renseignements personnels concernant les avantages discrétionnaires de ce genre.

De nombreuses raisons justifient donc la nécessité d'un critère comparatif quelconque. La loi canadienne reconnaît en fait cette nécessité puisque, à l'exception du droit d'accès limité aux données personnelles prévu par la Loi sur l'accès à l'information, toutes les autres communications doivent être faites en fonction d'un critère comparatif, quoiqu'il s'agisse purement dans ce cas d'une question de discrétion administrative. Il reste à s'interroger sur la meilleure façon de concevoir ce critère comparatif. Avant d'offrir quelques suggestions à cet égard, il nous semble utile de traiter de deux points préliminaires: premièrement, il faut souligner que l'on pourrait dans une certaine mesure résoudre le conflit entre la liberté de l'information et la protection de la vie privée en retranchant les noms des personnes identifiables avant de communiquer les documents demandés. Les données anonymes de ce genre satisferont fréquemment les exigences du demandeur et retarderont, voire élimineront complètement, les risques de violation de la vie privée. Toutefois, comme l'indique l'arrêt de principe rendu aux États-Unis dans

l'affaire U.S. Department of the Air Force v. Rose,⁹ la suppression des noms sur les documents peut faciliter la comparaison entre l'intérêt public et les risques de violation de la vie privée, même lorsqu'il subsiste un certain risque d'identification ou de violation de la vie privée d'une personne. Dans l'affaire Rose, des chercheurs juridiques qui faisaient une étude sur la discipline militaire avaient demandé à consulter des documents concernant les procédures disciplinaires de l'Armée de l'air. Ils avaient admis que les documents sans les noms des personnes impliquées seraient suffisants aux fins de leur étude, mais il leur fut répondu que, même si les noms étaient supprimés, il serait possible dans de nombreux cas à des personnes au courant des incidents en question d'identifier la personne à qui les mesures disciplinaires avaient été imposées. La Federal Court a décidé que, même si ce risque était réel, l'intérêt public prévalait en l'occurrence, et justifiait l'examen de cet aspect des activités gouvernementales par des personnes extérieures au gouvernement.

Dans tous les cas où la suppression des noms ou des autres détails particuliers permet d'éviter l'identification des individus, le demandeur devrait pouvoir se plier au principe de la divisibilité, c'est-à-dire le principe adopté dans les législations américaine et canadienne sur l'accès à l'information prévoyant que le gouvernement doit communiquer toute partie d'un document pouvant être raisonnablement extraite d'un document demandé qui n'est pas assujéti à l'une des exceptions. L'affaire Rose nous enseigne toutefois que, même si l'on ne peut ainsi éliminer la possibilité d'identification, il reste néanmoins possible de réduire les risques de violation de la vie privée à un point tel que les considérations d'intérêt public en faveur de l'accès à l'information acquièrent alors préséance.

Une deuxième question s'est posée dans les jugements américains où l'on a appliqué le critère de la "violation clairement injustifiée de la vie privée": on s'est demandé si l'on devait se fonder sur l'utilisation spécifique des données personnelles proposée par le demandeur pour décider si leur communication est justifiée dans l'intérêt public. Ainsi, lorsque le requérant demande les renseignements dans le cadre de recherches médicales ou d'un autre type de recherches très utiles, on doit comparer les avantages potentiels de cette recherche avec la violation de la vie privée; ou, étant donné que les données personnelles risquent d'être plus largement diffusées dans le public en raison de la communication, devrait-on ignorer l'utilisation particulière que le demandeur entend faire des données? Le débat sur cette question, aux États-Unis et dans les écrits qui y ont été publiés, a été provoqué par le jugement rendu dans l'affaire Getman v. NLRB¹⁰; des professeurs de droit spécialisés en relations de travail avaient pu obtenir les noms des syndiqués ayant voté en faveur de l'accréditation d'un syndicat, afin de faire une recherche sur certaines orientations du National Labour Relations Board des États-Unis en regard du processus d'accréditation. Dans l'affaire Getman, le tribunal a accueilli la demande spécifiquement pour les fins de ce projet, les demandeurs ayant dû s'engager à ne communiquer à personne les noms des syndiqués. Il est clair que la communication de ces noms au début du processus d'accréditation, à l'employeur ou au grand public, constituerait clairement une violation injustifiée de la vie privée. Dans l'affaire Getman, le tribunal était donc disposé à accorder un accès limité à l'information à ces demandeurs, même s'il avait été inapproprié de permettre ce même accès au grand public.

L'affaire Getman a suscité une vive controverse. Certains commentateurs se sont objectés à la décision, soutenant que l'on ne devrait pas tenir compte du "besoin de savoir" des demandeurs, puisque la Freedom of Information Act donne à "toute personne" un droit d'accès à l'information. D'autres justifiaient le principe de cette interprétation de la loi qui, à mon avis à tout le moins, est contraignante. Si l'on intègre le concept du "besoin de savoir" retenu dans certains jugements, celui-ci risque d'étendre son influence à toute la jurisprudence relative au conflit entre la liberté de l'information et la protection de la vie privée, et d'amoindrir considérablement l'efficacité du droit d'accès à l'information. En outre, il semble peu pratique d'adopter une pratique générale consistant à restreindre la communication secondaire des renseignements donnés aux demandeurs aux termes de la Freedom of Information Act. Il me semble qu'une bien meilleure solution, qui a d'ailleurs été proposée dans le rapport de la Commission de l'Ontario, consisterait à traiter l'accès à l'information à des fins de recherche comme un problème distinct, et à élaborer un mécanisme permettant l'accès aux données personnelles à des fins de recherche au profit de la collectivité.¹¹

Pour en venir maintenant à la question principale, c.-à-d. comment atteindre un équilibre entre la liberté de l'information et la protection de la vie privée, elle revient fondamentalement à se demander s'il est possible de faire mieux que de réitérer, aux personnes chargées de prendre ce genre de décisions, le critère général contenu dans les lois canadienne et américaine, mais formulé en termes sensiblement différents: elles

devraient comparer soigneusement les avantages et inconvénients respectifs des considérations d'intérêt public favorisant la communication des renseignements et ceux des considérations personnelles favorisant la protection de la vie privée. J'estime pour ma part que l'on peut substantiellement raffiner cette approche en essayant d'élaborer divers facteurs plus explicites, dont devrait tenir compte une personne qui s'efforce de concilier ces deux intérêts. Les propositions suivantes sont inspirées, pour l'essentiel, des commentaires semblables contenus dans le rapport de l'Ontario, et d'une récente relecture de la jurisprudence américaine où les tribunaux ont appliqué le critère de la "violation clairement injustifiée de la vie privée".

A mon avis, on devrait tenir compte des facteurs suivants lorsqu'on essaie de concilier ces intérêts contradictoires:

- a) L'accès à l'information est-il nécessaire pour permettre à un individu d'atteindre l'un des objectifs sous-jacents de la législation sur la liberté de l'information, c.-à-d. un examen efficace de l'activité des institutions gouvernementales, une participation réelle aux débats sur les affaires publiques et une plus grande équité dans les processus administratifs de prise de décision touchant les individus.

Comme je l'ai déjà mentionné, on ferait peut-être trop confiance à la nature humaine si l'on permettait aux fonctionnaires eux-mêmes de déterminer si une demande donnée permettrait d'atteindre ces objectifs. Toutefois, il ne s'agit pas là d'une question particulièrement difficile,

déterminer si une demande donnée permettrait d'atteindre ces objectifs. Toutefois, il ne s'agit pas là d'une question particulièrement difficile, et je pense qu'une tierce-partie pourrait y répondre avec une certaine assurance dans la plupart des cas.

- b) La demande d'accès à l'information est-elle susceptible de contribuer positivement à la santé ou à la sécurité publiques?

Outre les justifications politiques généralement acceptées mentionnées au point a), la communication de renseignements dans un tel but semble être considérée comme une retombée souhaitable de la législation sur la liberté de l'information, et constitue un motif particulièrement déterminant.

- c) L'accès à l'information en question permettrait-il de faire un choix plus éclairé lors de l'achat de biens et de services?

Une fois de plus, il semble s'agir d'une retombée incidente des mécanismes de liberté de l'information. On retrouve une certaine justification philosophique aux critères b) et c) à l'article 20 de la Loi sur l'accès à l'information du Canada, qui prévoit expressément la communication des résultats d'essais de produits ou d'essais d'environnement et, de façon plus générale, donne discrétion aux institutions gouvernementales pour communiquer des renseignements commerciaux si des raisons d'intérêt public (concernant la santé et la sécurité publiques, la protection de l'environnement) justifient le préjudice éventuellement causé à l'entité commerciale propriétaire des renseignements.

- d) La communication des renseignements sera-t-elle avantageuse pour la personne qu'ils concernent?

Il pourrait fort bien se présenter des situations où le seul objectif du demandeur consiste à faire bénéficier l'individu concerné d'un avantage quelconque; la communication des renseignements s'impose évidemment dans un tel cas. Le paragraphe 8(m) de la Loi sur la protection des renseignements personnels prévoit spécifiquement cette éventualité, qui justifie l'exercice du pouvoir discrétionnaire de communication. S'agit-il d'un genre de renseignement qui serait normalement communiqué dans d'autres circonstances?

Dans l'exemple 4 mentionné au début de ce document, nous nous sommes demandés si le public devrait avoir accès à des lettres écrites afin de justifier la mise en liberté d'un détenu. C'est le cas qui s'est présenté dans l'affaire Philadelphia Newspapers Inc. v. U.S. Department of Justice,¹² une décision rendue aux termes de la loi américaine, et dans laquelle le tribunal a statué que les lettres devraient être communiquées, puisque les personnes en question avaient, en un certain sens, témoigné de la réputation du détenu, ce qu'elles seraient normalement tenues de faire lors d'une audience publique. Dans un tel cas, comme pour toutes les autres analyses juridiques, une analogie féconde peut constituer un guide utile.

Par ailleurs, on peut tenir compte de plusieurs facteurs défavorables à la communication des renseignements:

- e) L'accès à l'information contreviendra-t-il aux objectifs du mécanisme juridique ayant initialement permis de recueillir les renseignements?

Il peut fort bien survenir des situations, lorsque la loi impose des procédures de conciliation par exemple, où la communication des renseignements empêcherait l'institution gouvernementale en question de s'acquitter efficacement des tâches que la loi lui impose. Il s'agirait certainement dans ce cas d'un argument puissant contre la communication.

- f) Les renseignements personnels ont-ils un caractère particulièrement confidentiel?

Il est possible de songer à certains types de renseignements, comme les renseignements médicaux ou les renseignements relatifs à l'admissibilité à des prestations de service social ou de bien-être social, dont la communication serait généralement perçue comme une violation particulièrement grave de la vie privée par les personnes concernées.

- g) Les renseignements sont-ils susceptibles d'être inexacts ou peu dignes de foi?

La probabilité que des données personnelles soient inexactes peut varier sensiblement en fonction des circonstances dans lesquelles elles ont été

recueillies ou fournies, ainsi que des garanties ou des procédures de vérifications adoptées par l'institution gouvernementale en question. La probabilité qu'on puisse diffuser des renseignements inexacts incitera sans aucun doute à ne pas communiquer les renseignements.

- h) Existe-t-il un risque que la personne concernée subisse un préjudice substantiel, de nature financière ou autre, en raison de la communication?

Certaines violations de la vie privée peuvent avoir pour effet, non seulement d'embarrasser l'individu concerné ou d'empiéter sur sa vie privée, mais également de lui causer un préjudice substantiel quelconque. Il s'agit là encore d'un facteur défavorisant la communication.

- i) Les renseignements ont-ils été fournis, de façon tacite ou expresse, sous le sceau de la confidentialité?

Un tribunal américain a suggéré que, bien qu'une promesse de confidentialité devrait fortement inciter à ne pas communiquer les renseignements, cela ne devrait être qu'un facteur à considérer pour déterminer si les renseignements doivent être communiqués au demandeur.¹³ Il y a tout lieu de penser qu'on devrait normalement respecter ce genre d'engagement, mais cela n'est pas certain dans les cas où, par exemple, l'individu qui a initialement fourni les renseignements n'avait pas vraiment pris l'engagement au sérieux, ou aurait pu être légalement obligé de fournir les renseignements en question.

Il est certain que l'expérience directe acquise dans l'application des mécanismes de liberté de l'information et de protection de la vie privée permettra de dégager d'autres principes de ce genre.

La Commission de l'Ontario a récemment recommandé une disposition législative relativement élaborée,¹⁴ prévoyant que plusieurs des propositions mentionnées ci-dessus seraient assimilées à des présomptions utilisées dans l'application du critère comparatif; j'avoue rester convaincu qu'il s'agit d'une solution attrayante aux problèmes exposés dans le présent document. À tout le moins, toutefois, il me semble que l'élaboration de principes de ce genre devrait faciliter la tâche des personnes qui doivent appliquer les normes plus vagues énoncées dans les législations américaine et canadienne.

La protection de la vie privée est une valeur importante, mais non absolue, qui doit être opposée aux autres valeurs comme celle, si largement acceptée de nos jours, de l'intérêt public à un libre accès aux renseignements détenus par le gouvernement. Lorsqu'ils ont fait face à la difficulté de concilier ces valeurs contradictoires, il semble que les rédacteurs légistes du système canadien aient reculé devant la tâche. Nous espérons que la présente analyse aidera dans une certaine mesure ceux qui doivent essayer de réaliser un équilibre satisfaisant entre l'accès à l'information et la protection de la vie privée, dans l'exercice de leurs pouvoirs discrétionnaires aux termes du paragraphe 8(m) de la Loi sur la protection des renseignements personnels.

Notes

- * Doyen, Osgoode Hall Law School, Université York. Droits d'auteur réservés.
1. 5 U.S.C. Section 552.
 2. Ibid., (b) 6.
 3. 5 U.S.C. Section 552a.
 4. Canada, Parlement, Première session, 32^e législature, 1980, Chambre des communes, Projet de loi C-43 (Loi édictant la Loi sur l'accès à l'information et la Loi sur la protection des renseignements personnels, modifiant la Loi sur la preuve au Canada et la Loi sur la Cour fédérale et apportant des modifications corrélatives à d'autres lois) adopté par la Chambre des communes, le 28 juin 1982, ci-après appelé la "Loi sur l'accès à l'information" ou la "Loi sur la protection des renseignements personnels".
 5. Loi sur la protection des renseignements personnels, article 3.
 6. Loi sur l'accès à l'information, paragraphe 19(2).
 7. 424 F. Supp. (1976).

8. Loi sur la protection des renseignements personnels, paragraphe 3 (j)
à (1) de la définition des "renseignements personnels".
9. 425 U.S. 352 (1976).
10. 450 F 2d 670 (DC Cir 1971).
11. Ontario Commission on Freedom of Information and Individual Privacy,
Final Report: Public Government for Private People (1980), vol. 2,
332-334.
12. 405 F Supp. 8 (ED Pa 1975).
13. Robles v. EPA, 484 F 2d 843 (4th Cir 1973).
14. Supra, note 11, pp. 335-338.

CA1
Z4
- 252

DOCUMENT: 870-123/010

INTERPROVINCIAL CONFERENCE ON PRIVACY:
INITIATIVES FOR 1984 (SYMPOSIUM)

Notes for an Address

The Honourable Norman Sterling, Q.C.
Provincial Secretary for
Resources Development



Toronto, Ontario
May 23-24, 1984

GOOD MORNING,

IT CERTAINLY IS A PLEASURE TO WELCOME YOU TO THE FIRST INTER-PROVINCIAL CONFERENCE ON COMPUTERS AND PRIVACY. IT IS LONG OVERDUE. I SAY THE FIRST, BECAUSE I BELIEVE THIS CONFERENCE IS UNIQUE IN THAT WE WILL BE EXPLORING ISSUES AND OPTIONS WHICH HAVE NEVER BEEN DISCUSSED IN A FORUM SUCH AS THIS BEFORE.

INDEED THE OVERWHELMING RESPONSE WHICH WE HAVE RECEIVED FOR THIS SYMPOSIUM IS MOST ENCOURAGING. IN FACT, CLOSE TO 300 MEMBERS OF THE INDUSTRIAL, MEDICAL AND BUSINESS COMMUNITIES ARE REPRESENTED HERE TODAY. THIS INDICATES TO ME THAT NOT ONLY ARE BUSINESSES AND GOVERNMENTS CONCERNED WITH THE PROBLEM, BUT THAT THIS COLLECTIVE INVOLVEMENT ALSO SIGNALS THE NEED FOR US AS A NATION, TO DEVELOP A UNIFORM APPROACH TO THE PRIVACY PROBLEM.

IN RECENT YEARS THE ISSUES SURROUNDING PRIVACY HAVE BEEN GREATLY ACCELERATED BY RAPIDLY CHANGING AND INCREASINGLY SOPHISTICATED TECHNOLOGY SYSTEMS.

THE ATTENDANCE HERE TODAY IS EVIDENCE THAT WE ARE ALL AFFECTED: GOVERNMENTS, CONSUMERS, BANKERS, MEDICAL PRACTITIONERS, AND SMALL AND LARGE BUSINESSES ALIKE.

YOU KNOW, IT IS SOMEWHAT IRONIC THAT ALTHOUGH WE AS CITIZENS VIEW PRIVACY AS SOMETHING PRECIOUS - SOMETHING WHICH WE CHERISH AND GUARD CLOSELY - THERE HAS NEVER BEEN ADEQUATE LEGAL RECOGNITION OR PROPER SAFEGUARDS TO ENSURE THIS RIGHT.

OH, I'M AWARE THAT THERE ARE SOME LIMITED PRIVACY ACTS IN EXISTENCE; AND THAT THE FEDERAL GOVERNMENT HAS PROPOSED CHANGES TO THE CRIMINAL CODE WHICH WILL SPECIFICALLY ADDRESS COMPUTER CRIME. BUT IT IS IMPORTANT TO REMEMBER THAT THESE CHANGES WILL ONLY ADDRESS THE BLATANT ABUSES OF SECURITY - THE HORROR STORIES WHICH WE OCCASIONALLY READ ABOUT IN THE PAPERS.

FOR EXAMPLE, ONE OF THE MOST EXTREME CASES OF ABUSE WHICH I HAVE HEARD RECENTLY INVOLVED A YOUNG MAN WHO WAS ABLE TO USE HIS HOME COMPUTER TO GAIN ACCESS, AND CONSEQUENTLY CHANGE THE BILLING STRUCTURE OF OVER 6,000 RADIATION THERAPY RECORDS OF PATIENTS AT A CANCER CENTRE IN MANHATTAN.

IN ONE RESPECT, THIS INCURSION INTO PRIVACY IS ALARMING. YET, BECAUSE THE EXAMPLE ILLUSTRATES SUCH A BLATANT BREACH OF SECURITY, IT WILL, IN MANY RESPECTS, BE MUCH EASIER FOR LEGISLATORS TO ADDRESS. THE CRIMINAL CODE AMENDMENTS ARE HOWEVER ONLY A VERY SMALL STEP.

THE LARGER, MUCH BROADER ISSUE AT STAKE IS THE CURRENT FREE-WHEELING EXCHANGE AND SELLING OF INFORMATION VIA ELECTRONIC MEANS WHICH POSES PERHAPS THE GREATEST CHALLENGE TO PRIVACY.

UNFORTUNATELY, THE CANADIAN EMPHASIS APPEARS TO BE ON MODIFYING EXISTING LEGISLATION. I BELIEVE, HOWEVER, THAT THAT IS SIMPLY NOT ENOUGH. IT IS NOW NECESSARY TO LOOK AT DEVELOPING STANDARDS THAT WILL DEAL DIRECTLY WITH THE MUCH MORE SUBTLE AND BROADER PROBLEM OF DATA CONTROL.

WHILE I DO NOT WISH TO OVER-DRAMATIZE THE SITUATION, I THINK RALPH NADER PUT IT WELL WHEN HE SAID IN 1971, "IT IS A RARE AMERICAN WHO DOES NOT LIVE IN THE SHADOW OF HIS DOSSIER....WHAT THE MISUSE OF COMPUTERS IS DOING AND CAN DO TO AN INDIVIDUAL'S FREEDOM (CONSTITUTES) A WARNING OF A NEW FORM OF SLAVERY."

CLEARLY, THIS ORWELLIAN VISION HAS NOT BECOME THE REALITY WHICH NADER STATES.

ON THE OTHER HAND WHAT HAS OCCURRED IS MUCH MORE SUBTLE, YET NONE THE LESS EQUALLY IMPORTANT. AT PRESENT, THERE IS NO RECOURSE FOR THE INDIVIDUAL WHO FEELS THAT THE INFORMATION HE HAS SUPPLIED HAS BEEN USED WITHOUT HIS AUTHORIZATION. IN THAT SENSE, PERHAPS WE HAVE BECOME SLAVES TO TECHNOLOGY.

WHEN AN INDIVIDUAL PROVIDES INFORMATION HE DOES SO FOR A SPECIFIC PURPOSE. HE DOES NOT DO IT WITH THE KNOWLEDGE THAT THE COURSE FOR THIS INFORMATION HAS ONLY BEGUN WHAT IS PROBABLY A LONG JOURNEY INTO A NEBULOUS STATE OF FREE-FLOWING DATA.

TO ILLUSTRATE MY POINT, I WILL REFER TO THE SOMEWHAT SIMPLISTIC YET COMPELLING CASE OF SUBSCRIBER LISTS. I AM SURE EVERYONE HERE CAN RELATE TO WHAT HAPPENS SHOULD YOU DECIDE TO SUBSCRIBE TO A PARTICULAR SERVICE. BEFORE YOU KNOW IT, YOU FIND YOU ARE RECEIVING AN EXTRAORDINARY AMOUNT OF "INVITATIONS" TO JOIN EVERY OTHER SERVICE, WHICH MAY OR MAY NOT BE EVEN REMOTELY RELATED TO THE ORIGINAL SUBSCRIPTION. CHANCES ARE, YOU ARE ANNOYED - BUT WHAT CAN YOU DO? YOUR PRIVACY, ALTHOUGH INVADED, HAS NOT CAUSED ANY DIRECT HARM. SO YOU TOSS THE "INVITATIONS" AND CONTINUE WITH YOUR DAILY LIFE.

THE NAGGING QUESTION THOUGH - WHICH NEVER SEEMS TO BE ANSWERED IS: HOW DID "THOSE" PEOPLE GET MY NAME, AND ADDRESS?; HOW DO "THEY" KNOW MY PERSONAL PREFERENCES?; WHAT ELSE DO "THEY" KNOW?; WHAT ELSE ARE "THEY" CAPABLE OF FINDING OUT?; AND MOST IMPORTANT - HOW DO I STOP THIS?; WHO DO I COMPLAIN TO?

I DO NOT BELIEVE, THAT INDUSTRY'S MOTIVES ARE SINISTER. RATHER I BELIEVE THAT MOST COMPANIES HANDLE CONSUMER INFORMATION IN A RESPONSIBLE MANNER. THE PRIMARY MOTIVE IS QUITE SIMPLY ONE OF ECONOMICS. THERE IS A GREAT DEAL OF MONEY TO BE GAINED FROM THE SELLING OF INFORMATION. AND, THERE ISN'T ANYTHING INHERENTLY WRONG WITH THAT MOTIVE IN ISOLATION.

THE POINT I WISH TO STRESS, IS NOT THE FACT THAT THE INFORMATION IS SOLD. THAT IS ONLY THE TIP OF THE ICEBERG. RATHER, IT IS THE END RESULT WHICH HAS - INADVERTENTLY PRODUCED A MATTER OF GREAT CONCERN - NAMELY, A CITIZEN'S RIGHT TO PRIVACY.

THE COMPLEXITY OF THIS ISSUE IS COMPOUNDED WHEN THE INFORMATION BEGINS TO CROSS BORDERS, WHETHER THEY BE PROVINCIAL OR INTERNATIONAL. COMMONLY REFERRED TO AS TRANS-BORDER DATA FLOW - THE EMPHASIS SHOULD BE PLACED ON THE WORD "BORDER". THE CURRENT ELECTRONIC AGE WHICH WE ALL FIND OURSELVES IN IS MAKING THOSE BORDERS INCREASINGLY FLUID. THE LINES ARE NO LONGER DISTINCT; THEY HAVE BECOME BLURRED.

THIS BLURRINESS HAS MADE IT IMPOSSIBLE FOR ANY ONE JURISDICTION TO ADDRESS THE PRIVACY ISSUE IN ISOLATION. THE NECESSITY FOR A COORDINATED AND COMPARABLE APPROACH HAS BEEN RECOGNIZED BY THE COUNCIL OF EUROPE.

IN 1981, IN STRASBOURG, FRANCE, THE COUNCIL ADOPTED A DATA PROTECTION CONVENTION. THE RECOMMENDATIONS WERE SIGNED BY 16 PARTICIPATING COUNTRIES.

WHEN THIS CONVENTION COMES INTO FORCE IT WILL CONFIRM THE RIGHT OF COUNTRIES WITH DATA PROTECTION LEGISLATION TO REFUSE TO ALLOW PERSONAL INFORMATION TO BE SENT TO OTHER COUNTRIES WHICH DO NOT HAVE COMPARABLE SAFEGUARDS. THIS COULD THREATEN INDUSTRIES WITH INTERNATIONAL INTERESTS OPERATING IN ONE COUNTRY, BUT WHICH PROCESS DATA FOR CUSTOMERS IN MANY DIFFERENT NATIONS.

AT PRESENT, FOUR COUNTRIES - SWEDEN, FRANCE, SPAIN AND NORWAY HAVE RATIFIED THE CONVENTION. IN OTHER WORDS, THEY HAVE NOT MERELY SIGNED IT, BUT HAVE ENACTED LEGISLATION. IN ADDITION, THE UNITED KINGDOM HAS FORMALLY STATED ITS INTENTION TO RATIFY, AS SOON AS THE DATA PROTECTION BILL IS PASSED BY PARLIAMENT. THE BILL WHICH RECEIVED 2ND READING LAST MARCH IS EXPECTED TO BE PASSED THIS SUMMER. A TOTAL OF FIVE COUNTRIES ARE REQUIRED BEFORE THE ARTICLES OF THE CONVENTION CAN TAKE EFFECT.

THE LEGISLATION PROPOSED BY THE UNITED KINGDOM IS INTERESTING IN THAT IT ENCOMPASSES BOTH THE PRIVATE AND PUBLIC SECTORS. THE CENTRAL FEATURE BEHIND THIS INITIATIVE IS THE ESTABLISHMENT OF A DATA PROTECTION REGISTRAR AND TRIBUNAL. IN THIS RESPECT ALL USERS OF ELECTRONIC DATA SYSTEMS, WITH SOME EXCEPTIONS, MUST REGISTER. THE REGISTRAR WOULD BE EMPOWERED TO EXAMINE ALLEGED CASES OF MISUSE AND SUBSEQUENTLY "DE-REGISTER" DATA BANKS WHICH CONTRAVENE DATA - PROTECTION PRINCIPLES.

AS WELL, THE DATA PROTECTION REGISTRAR CAN PROHIBIT THE TRANSFER OF DATA OUTSIDE THE UNITED KINGDOM WHERE THE COUNTRY OF DESTINATION FAILS TO MEET MINIMUM DATA PROTECTION STANDARDS. THE DIRECT IMPLICATIONS OF THIS LAST POINT COULD INDEED BE TREMENDOUS FOR CANADIAN COMPANIES WHO DO BUSINESS WITH THE UNITED KINGDOM. TO ILLUSTRATE THE POTENTIAL IMPACT, IN ONTARIO, NEARLY 20 PERCENT OF OUR WORK FORCE -- MORE THAN 800,000 PEOPLE -- DEPEND ON EXPORT-RELATED ACTIVITIES FOR THEIR JOBS. IN 1982, 40% OF THE ONTARIO JOBS IN THE MANUFACTURING SECTOR DEPENDED ON SALES OUTSIDE CANADA.

THE HARD FACT LADIES AND GENTLEMEN IS THAT UNLESS WE DEVELOP GUIDELINES GOVERNING DATA PROTECTION, FUTURE TRADE DISCUSSIONS COULD INDEED BE AFFECTED.

TO SUM UP, THE ISSUES WE WILL BE DISCUSSING DURING THE NEXT TWO DAYS ARE FAR-REACHING. FOR THE MATTER OF PRIVACY HAS, IN EFFECT, ALSO BECOME A MATTER OF ECONOMY. AS GOVERNMENTS, WE MUST ADDRESS THE CONCERNS SURROUNDING THE PROTECTION OF INDIVIDUAL PRIVACY AND GENERAL ACCESS RIGHTS.

FOR INDUSTRY, IT BECOMES A BIT OF A JUGGLING ACT: THESE SAME CONCERNS MUST BE FURTHER BALANCED AGAINST A NEED FOR INFORMATION, IN CONJUNCTION WITH THE COST OF IMPLEMENTING PRIVACY SAFEGUARDS.

IN ONTARIO WE HAVE EXAMINED THE QUESTIONS OF PRIVACY VS ACCESS AND HAVE TRIED TO STRIKE THE DIFFICULT YET VITAL BALANCE BETWEEN THE TWO IN THE PUBLIC SECTOR.

ONTARIO'S PROPOSED PRIVACY AND ACCESS LEGISLATION IS FOCUSED ON THE DEVELOPMENT OF FAIR INFORMATION PRACTICES FOR GOVERNMENT DATA BANKS. THE ESTABLISHMENT OF A PRIVACY AND INFORMATION COMMISSIONER WILL PROVIDE CITIZENS WITH AN APPEAL MECHANISM CONCERNING THE RELEASE OR PROTECTION OF DOCUMENTS.

IN ADDITION, THE FORMATION OF A DATA PROTECTION OFFICE, IS ALSO PROPOSED IN THE BILL. THE PRINCIPLE THRUST AND MANDATE BEHIND THIS NEW INITIATIVE WILL BE TO PROVIDE INTERNAL GUIDELINES AND TO ACT AS A PRIVACY "WATCH DOG" WITHIN GOVERNMENT.

SO, WHAT THEN ARE THE OPTIONS FOR CANADA? ENCLOSED IN THE CONFERENCE KIT IS A DISCUSSION PAPER ON PRIVACY.

ESSENTIALLY, THE PAPER EXAMINES VARIOUS OPTIONS AND POSSIBLE INITIATIVES WHICH COULD BE INTRODUCED BY BOTH THE PUBLIC AND PRIVATE SECTORS.

THERE ARE FOUR POSSIBLE ROUTES WHICH WE CAN EXPLORE. ONE, A VOLUNTARY PRIVACY CODE, WHICH I JUST REFERRED TO; TWO, A LEGISLATED PRIVACY CODE; THREE, A SYSTEM OF REGISTRATION AND REGULATION; AND FOUR, AN APPROACH WHICH COMBINES ELEMENTS OF THE FIRST THREE.

THIS LIST IS CLEARLY NOT AN EXHAUSTIVE ONE. BUT I SUSPECT THAT IT DOES OFFER SOME "FOOD FOR THOUGHT" AND WILL PROVIDE FOR CONSIDERABLE DISCUSSION DURING THE NEXT TWO DAYS.

FROM THE INDIVIDUAL CITIZEN'S POINT OF VIEW, THE THREAT OF PRIVACY OF PERSONAL INFORMATION EXISTS IN BOTH SECTORS. THUS FAR, HOWEVER, NORTH AMERICAN PRIVACY LAWS HAVE ONLY ADDRESSED THE ISSUE IN THE PUBLIC SECTOR.

THE NEED TO BROADEN THE SCOPE AND TO ESTABLISH STANDARDS BECOMES READILY APPARENT WHEN ONE SEES THAT COMPANIES WITH VOLUNTARY PRIVACY CODES ARE STILL THE EXCEPTION RATHER THAN THE RULE. IT IS CLEAR, THAT THE INCREASING AND WIDESPREAD USE OF COMPUTERIZED INFORMATION REQUIRES SOME SAFEGUARDS. THESE SAFEGUARDS MUST ENSURE THAT AN INDIVIDUAL'S RIGHT TO PRIVACY IS NOT INFRINGED UPON.

THE VOLUNTARY CODE, ALLOWS INDUSTRY MAXIMUM FLEXIBILITY TOWARDS THE INCORPORATION OF DATA PROTECTION STANDARDS. IT WOULD ALSO BE ADAPTABLE TO CHANGING TECHNOLOGY AND PUBLIC REQUIREMENTS. COMPANIES SUCH AS WARNER AMEX CABLE IN THE U.S., AND IBM IN EUROPE HAVE ALREADY DEVELOPED GUIDELINES FOR THE PROTECTION OF PERSONAL INFORMATION IN THEIR FILES. IN CANADA, IT IS MY UNDERSTANDING THAT THE CANADIAN CABLE TELEVISION ASSOCIATION IS IN THE PROCESS OF DEVELOPING A PRIVACY CODE.

WHILE SUCH RESPONSIBLE CORPORATE ACTION IS COMMENDABLE, A UNIFORM APPROACH MAY BE NECESSARY TO ADDRESS PRIVACY PROBLEMS. CLEARLY THE ADOPTION OF VARIOUS VOLUNTARY CODES, BY DIFFERENT SECTORS, COULD RESULT IN A PATCH-WORK APPROACH.

A COMPROMISE BETWEEN THE VOLUNTARY CODE AND THE MORE TRADITIONAL GOVERNMENT REGULATORY SOLUTIONS LIES IN THE LEGISLATIVE ROUTE. IN ESSENCE, A GOVERNMENT COULD SET OUT FAIR INFORMATION PRACTICES WHICH WOULD ALSO INCLUDE A SANCTION FOR THE VIOLATION OF THOSE PRACTICES. THIS LAW WOULD ESSENTIALLY ALLOW FOR SELF REGULATION OF INDUSTRY AND WOULD PERMIT LEGAL REMEDY.

WHILE THIS OPTION DOES CONTAIN SOME BENEFITS, IT DOES NOT REALLY PROVIDE A PRACTICAL SOLUTION. REALISTICALLY SPEAKING, I DON'T THINK MANY INDIVIDUALS WOULD UNDERTAKE THE TIME AND COST THAT IS INVOLVED IN PURSUIT OF A CIVIL LAWSUIT.

ON THE OTHER SIDE OF THE COIN EXISTS THE OPTION OF COMPLETE REGISTRATION AND REGULATION. THIS BASICALLY IS THE APPROACH WHICH HAS BEEN TAKEN IN THE UNITED KINGDOM DATA PROTECTION BILL. ESSENTIALLY, GOVERNMENT WOULD BE EMPOWERED TO: GIVE INDIVIDUALS DEFINED RIGHTS TO ACCESS AND CORRECTION; REGULATE THE COLLECTION AND THIRD PARTY DISCLOSURE OF PERSONAL INFORMATION, AND GUARANTEE THE SECURITY OF DATA BY ESTABLISHING A REGISTRAR WITH INVESTIGATION AND ENFORCEMENT RESPONSIBILITIES. IN SHORT THE COLLECTION OF PERSONAL INFORMATION IN AN ELECTRONIC DATA BANK BECOMES A PRIVILEGE AND NOT A RIGHT.

THE FOURTH APPROACH IS A COMBINATION OF THE THREE I HAVE JUST DISCUSSED. ESSENTIALLY IT INVOLVES A COMBINATION OF SELF REGISTRATION AND REGULATION.

ASSOCIATIONS WOULD BE ENCOURAGED TO DEVELOP PRIVACY CODES TAILORED TO THEIR INDUSTRY. AN INTERNAL MONITORING SYSTEM WOULD BE A VERY POSITIVE FORCE TOWARDS ENSURING COMPLIANCE AMONG INDUSTRY. IN COOPERATION WITH A PUBLIC PRIVACY OFFICE, A REGISTRY COULD BE MAINTAINED OF ALL PARTICIPATING ASSOCIATIONS AND COMPANIES.

I THINK IT IS IMPORTANT, TO STRESS THAT GOVERNMENTS MUST NOT OVER-REACT. INDUSTRY MUST BE ALLOWED THE OPPORTUNITY TO RESPOND TO THESE NEW CHALLENGES IN A REASONABLE AND RESPONSIBLE MANNER. BEFORE WE ALL EMBARK ON AN "ANTI '1984' CRUSADE", LET'S EXAMINE THE ALTERNATIVES CLOSELY.

I AM CONFIDENT THAT GIVEN THE OPPORTUNITY AND THE INTEREST SHOWN HERE TODAY, BY BOTH THE PUBLIC AND PRIVATE SECTORS, WE WILL BE ABLE TO FURTHER OUR DIALOGUE IN A MEANINGFUL AND CONSTRUCTIVE FASHION.

THANK YOU.

CA1

Z2

-C52

DOCUMENT: 870-123/010

CONFÉRENCE INTERPROVINCIALE SUR LA PROTECTION
DES RENSEIGNEMENTS PERSONNELS : MESURES POUR 1984 (COLLOQUE)

Notes préparées pour une allocution

L'Honorable Norman Sterling, C.R.
Secrétaire provincial au
Développement des ressources



Toronto (Ontario)
Les 23 et 24 mai 1984

Bonjour,

Il me fait plaisir de vous souhaiter la bienvenue à la première conférence interprovinciale sur l'Informatique et le respect de la vie privée. Il s'agit en effet d'un événement fort attendu depuis longtemps. Je dis bien la première parce que je crois que cette conférence est unique en ce que nous aborderons des questions et des options qui n'ont jamais été discutées auparavant dans un forum comme celui-ci.

La participation à ce symposium, d'ailleurs fort élevée, est très encourageante. En effet, près de 300 membres du monde industriel, médical et des affaires y sont représentés. Cette réunion de personnes de divers milieux indique à mon avis que les entreprises et les gouvernements ne sont pas les seuls à se préoccuper de ce problème; cet intérêt généralisé indique qu'il nous faut en tant que nation, développer une approche uniforme au problème du respect de la vie privée.

Au cours des quelques dernières années, les questions ayant trait au respect de la vie privée ont pris beaucoup d'ampleur en raison du changement rapide et de la complexité accrue des systèmes technologiques.

L'assistance ici indique bien que nous sommes tous affectés qu'il s'agisse des gouvernements, des consommateurs, des banquiers, des médecins, des petites et des grandes entreprises.

Il est quelque peu ironique de constater que bien que nous, en tant que citoyens, considérons le respect de la vie privée comme une chose précieuse - une chose qui nous est chère et que l'on surveille de près - il n'y a jamais eu reconnaissance juridique adéquate ou adoption de garanties pour protéger ce droit.

Je reconnais qu'il existe des lois, bien que limitées, sur le respect de la vie privée; et que le gouvernement fédéral a proposé des changements au Code criminel portant précisément sur le délit informatique. Mais il importe de ne pas oublier que ces changements n'ont trait qu'aux délits flagrants portant atteinte à la sécurité comme c'est le cas des histoires effroyables qui apparaissent à l'occasion dans les journaux.

Par exemple, un cas extrême à cet égard dont j'ai eu connaissance récemment fait état d'un jeune homme qui, au moyen de son ordinateur à domicile a réussi à avoir accès à plus de 6,000 dossiers de patients subissant une radiothérapie dans un institut cancérologique à Manhattan et à en modifier la structure de facturation.

D'une part, cette ingérence dans la vie privée constitue un fait alarmant. Or, c'est précisément parce que ce délit est flagrant qu'il sera facile aux législateurs de s'attaquer à cette question. Les modifications au Code criminel ne représentent toutefois qu'une très petite étape.

La grande question qui est en jeu est l'échange et la vente d'informations actuels par des moyens électroniques, ce qui pose peut-être bien la plus grande menace au respect de la vie privée.

Malheureusement, il semblerait que le Canada ne compte que modifier la législation existante. Je trouve cependant que cette démarche est insuffisante. Il importe à l'heure actuelle d'examiner les principes qui sont en train de se développer et qui abordent directement la question plus subtile et plus étendue du contrôle des données.

Bien que je n'aie nullement l'intention de dramatiser à outrance la situation, je crois que Ralph Nader exprime bien les choses lorsqu'il déclare en 1971: "Il est rare qu'on trouve un Américain qui ne vit pas dans l'ombre de son dossier... Ce que le mauvais usage des ordinateurs est en train de faire et peut faire à la liberté de l'individu (constitue) un avertissement d'une nouvelle forme d'esclavage."

Il est clair que cette vision orwellienne n'est pas devenue la réalité décrite par Nader.

D'autre part, la situation est beaucoup plus subtile, bien que tout aussi importante que celle décrite par Nader. A l'heure actuelle, il n'y a aucun recours pour l'individu qui croit que les informations qu'il a fournies ont été utilisées sans son autorisation. En ce sens, nous sommes peut-être bien devenus esclaves de la technologie.

Lorsqu'un individu donne des informations, il le fait dans un but précis tout en ne se rendant pas compte que le parcours de ces informations ne fait que commencer et qu'il s'agira probablement d'un long trajet dans un état nébuleux de données circulant librement.

Le cas des listes de souscription quelque peu simpliste bien que convaincant illustre bien mon point. Je suis certain que vous pouvez vous imaginer ce qui se passe lorsque vous décidez de souscrire à un service particulier. Avant même que vous vous en rendiez compte, vous avez reçu une quantité extraordinaire "d'invitations" vous incitant à vous joindre à toutes sortes de services reliés de loin ou même pas reliés de loin à la première souscription. Vous serez probablement vexé, mais que pouvez-vous faire? Votre vie privée, bien qu'il y ait eu ingérence, n'a pas été atteinte directement. Alors vous mettez les "invitations" de côté et continuez à vivre votre vie.

La question qui ne fait que revenir et qui ne semble jamais obtenir de réponse est: Comment "ces" personnes obtiennent-elles mon nom et mon adresse?; Comment connaissent-elles mes préférences personnelles?; Que savent-elles d'autre?; Quelles autres choses peuvent-elles trouver?; et ce qui importe le plus - comment puis-je mettre fin à cela?; A qui dois-je me plaindre?

Je ne crois pas que les motifs des entreprises sont malfaisants. Je crois plutôt que la plupart des compagnies gèrent les informations sur les consommateurs de façon responsable. Le motif premier est tout simplement d'ordre économique. Il y a beaucoup d'argent à tirer de la vente d'informations. Il n'y a pas de mal à cela comme tel.

Le point que je voudrais souligner n'est pas le fait que les informations sont vendues. La vente d'informations ne représente que la partie émergée de l'iceberg. Il s'agit plutôt du résultat final qui, par inadvertance, a entraîné un problème important à savoir, le droit du citoyen au respect de sa vie privée.

La complexité de cette question s'accroît lorsque les informations commencent à traverser les frontières, qu'il s'agisse de frontières provinciales ou internationales. Ce phénomène est communément appelé le flux transfrontière de données - le mot "frontière" revêt ici le plus d'importance. L'ère électronique dans laquelle nous vivons tous est en train de rendre ces frontières de plus en plus fluides. Les lignes ne sont plus distinctes; elles sont embrouillées.

Cet embrouillement a fait en sorte qu'il est impossible pour un Etat d'aborder la question du respect de la vie privée de façon isolée. Le Conseil de l'Europe a reconnu la nécessité de concevoir une approche coordonnée et comparable.

En 1981, à Strasbourg en France, le Conseil de l'Europe a adopté une Convention relative à la protection des données. Les recommandations ont été signées par 16 pays participants.

Cette Convention une fois en vigueur aura pour effet de sanctionner le droit des pays ayant une législation en matière de protection des données de refuser la transmission d'informations relatives aux personnes à d'autres pays n'ayant pas de garanties comparables. Une telle mesure pourrait nuire aux entreprises qui fonctionnent dans un pays quelconque tout en ayant des intérêts internationaux et qui effectuent le traitement des données des clients dans divers pays.

A l'heure actuelle, quatre pays ont ratifié la Convention soit la Suède, la France, l'Espagne et la Norvège. En d'autres mots, ils n'ont pas fait que signer la Convention, ils ont promulgué une législation. De plus, le Royaume-Uni a formellement déclaré son intention de ratifier la Convention dès que le Projet de loi sur la protection des données aura été adopté par le Parlement. Le projet de loi qui en était à sa deuxième lecture en mars dernier est supposé être adopté cet été. Il faut un total de cinq pays pour que les articles de la Convention prennent effet.

La législation proposée par le Royaume-Uni est intéressante en ce qu'elle englobe le secteur privé et le secteur public. La caractéristique centrale de cette initiative est l'établissement d'un Greffier et d'un Tribunal relatif à la protection des données. A cet égard, tous les utilisateurs des systèmes de données électroniques, à raison de quelques exceptions, doivent s'enregistrer. Le Greffier est habilité à examiner les prétendus cas de mauvais usage et par la suite à "radier" les banques de données qui ont enfreint les principes relatifs à la protection des données.

Le Greffier responsable de la protection des données peut également empêcher le transfert de données en dehors du Royaume-Uni si le pays de destination ne s'est pas conformé aux normes minimales régissant la protection des données. Les implications directes de ce dernier point pourraient en effet être énormes pour les compagnies canadiennes qui font affaire avec le Royaume-Uni. Pour illustrer l'impact qu'une telle situation pourrait avoir, il faut considérer qu'en Ontario, près de 20 pour cent de notre main-d'oeuvre - soit plus de 800,000 personnes - dépendent des activités reliées à l'exportation pour ce qui est de leur emploi. En 1982, 40% des emplois en Ontario dans le secteur manufacturier dépendent des ventes en dehors du Canada.

Mesdames et messieurs, il est incontestable qu'à moins de développer certaines lignes de conduite en matière de protection des données, les discussions sur le commerce futur pourraient en être affectées.

En résumé, les questions dont nous discuterons au cours des deux prochains jours sont d'une portée considérable puisque le problème du respect de la vie privée est devenu un problème d'ordre économique. En tant que gouvernements, il nous faut nous attaquer aux problèmes qui concernent la protection de la vie privée de l'individu ainsi que les droits d'accès généraux aux informations.

Pour les entreprises, il s'agit un peu d'un numéro de jonglerie puisqu'il existe un certain conflit entre la protection de la vie privée, le besoin d'information et le coût d'implantation des garanties en matière de respect de la vie privée.

En Ontario, nous avons examiné les questions du respect de la vie privée par opposition à l'accès aux données et avons tenté d'en arriver au juste milieu dans le cadre du secteur public.

La législation proposée par l'Ontario en matière de respect de la vie privée et d'accès à l'information est axée sur le développement de méthodes d'information justes pour les banques de données du gouvernement. L'établissement d'un Commissaire responsable de la protection de la vie privée et de l'accès à l'information fournira aux citoyens un mécanisme d'appel concernant la divulgation ou la protection de documents.

Le projet de loi propose également la création d'un Bureau de protection des données. Le but principal et le mandat de ce bureau sont de prévoir des lignes de conduite internes et d'agir en tant que "chien de garde" en ce qui a trait au respect de la vie privée au sein du gouvernement.

Quelles sont donc les options pour le Canada? Vous trouverez dans le dossier de la conférence un document de travail sur le respect de la vie privée.

Essentiellement, le document de travail examine les diverses options et initiatives possibles qui pourraient être introduites par les secteurs public et privé.

Nous pouvons y distinguer quatre voies possibles. La première, un code volontaire du respect de la vie privée que je viens de mentionner; la deuxième, un code de lois sur le respect de la vie privée; la troisième, un système d'enregistrement et de réglementation; et la quatrième, une approche qui englobe les éléments des trois premières voies.

Il ne s'agit certes pas d'une liste exhaustive. Mais j'ai l'impression qu'elle donnera "matière à réflexion" et entraînera de nombreuses discussions au cours des deux prochains jours.

Du point de vue du citoyen, le danger au niveau du secret des informations relatives aux personnes existe dans les deux secteurs. Jusqu'ici les lois sur le respect de la vie privée en Amérique du Nord ne traitent de la question que dans le cadre du secteur public.

Le besoin d'élargir la portée des mesures et d'établir des normes devient tout de suite apparent lorsque l'on considère que les compagnies s'étant dotées de codes volontaires en matière de respect de la vie privée constituent toujours l'exception plutôt que la règle. Il est clair que l'utilisation répandue et sans cesse croissante de données informatiques nécessite certaines garanties. Ces garanties doivent protéger le droit de l'individu contre toute atteinte au respect de sa vie privée.

Le code dit volontaire comporte une flexibilité maximale pour les entreprises en ce qui a trait à l'incorporation des normes de protections des données. Il serait également adaptable à la technologie toujours changeante et aux exigences du public. Certaines compagnies comme Warner Amex Cable aux Etats-Unis et IBM en Europe ont déjà établi certaines lignes de conduite en vue de protéger les informations relatives aux personnes dans leurs dossiers. Au Canada, je crois comprendre que l'Association canadienne de câblodistribution est en train de mettre sur pied un code de protection de la vie privée.

Bien qu'une telle mesure constitue un geste responsable qui mérite d'être loué, il importe néanmoins de concevoir une approche uniforme pour faire face aux problèmes relatifs au respect de la vie privée. Il est clair que l'adoption de divers codes volontaires, selon les secteurs, donnerait lieu à une certaine incohérence.

Le moyen législatif constitue un compromis entre le code volontaire et les solutions traditionnelles de réglementation gouvernementale. Essentiellement, le gouvernement établirait des procédures en matière d'information en vertu desquelles des sanctions seraient prévues en cas d'infraction à celles-ci. Cette loi permettrait l'auto-réglementation des entreprises et l'exercice d'un droit en justice.

Bien que cette option comporte certains avantages, elle ne constitue pas vraiment une solution pratique. En fait, je ne crois pas qu'il y aurait bien des personnes prêtes à consacrer le temps et l'argent nécessaires afin d'exercer une poursuite judiciaire.

Il existe d'autre part l'option d'enregistrement et de réglementation complets. Il s'agit en effet de l'approche adoptée dans le Projet de loi sur la protection des données au Royaume-Uni. Essentiellement, le gouvernement a le pouvoir: de donner aux individus des droits définis en ce qui a trait à l'accès aux informations et à la correction de celles-ci; de réglementer la collecte et la divulgation à des tiers des informations relatives aux personnes, et de garantir la sécurité des données en établissant un greffier responsable des investigations en matière de protection de la vie privée et du respect de la loi. Bref, la collecte d'informations sur les personnes dans une banque de données électroniques devient un privilège et non un droit.

La quatrième approche est une combinaison des trois autres dont je viens de discuter. Elle englobe essentiellement le phénomène de l'auto-réglementation et de la réglementation.

Les associations seraient encouragées à établir des codes de protection de la vie privée conçus en fonction de leur industrie. Un système de surveillance interne serait un moyen efficace de faire respecter le code au sein de l'industrie. Un registre de toutes les associations et compagnies pourrait être maintenu en collaboration avec un Bureau public de protection de la vie privée.

Il importe que les gouvernements ne réagissent pas avec excès. Il faut accorder au monde industriel l'occasion de réagir à ces nouveaux défis de façon raisonnable et responsable. Avant d'entreprendre une "croisade anti 1984", nous devrions d'abord examiner les possibilités de près.

Compte tenu de la sollicitude et de l'intérêt manifestés ici par les secteurs public et privé, j'ai bon espoir que nous serons capables de poursuivre notre dialogue de façon significative et constructive.

Merci.

DOCUMENT: 870-123/011

INTERPROVINCIAL CONFERENCE ON PRIVACY:
INITIATIVES FOR 1984 (SYMPOSIUM)

Access to Information & Barriers for Privacy:
The Search for Balance

T. Murray Rankin
Faculty of Law
University of Victoria



Toronto, Ontario
May 23-24, 1984

A. INTRODUCTION

HISTORICALLY, DATA PROTECTION LAWS AND FREEDOM OF INFORMATION LAWS TRACE THEIR ROOTS TO DIFFERENT SOURCES. THEY EMERGED AT VERY DIFFERENT TIMES IN EUROPEAN HISTORY INITIALLY IN RESPONSE TO DIFFERENT PERCEIVED PROBLEMS. AT PRESENT, HOWEVER, THESE TWO SEPARATE LEGAL CLAIMS HAVE BEEN BLURRED IN MANY PEOPLE'S EYES. I WILL ARGUE THAT THIS BLURRING IS A CONSEQUENCE OF THE RECENT TECHNOLOGICAL ACHIEVEMENTS WHICH ARE CREATING OUR GLOBAL "INFORMATION SOCIETY". THE OVERLAPPING OF THESE TWO LEGISLATIVE REGIMES MAY FORESHADOW THE EVENTUAL CREATION OF A COMPREHENSIVE "INFORMATION LAW" AS OUR LEGAL RULES DEVELOP IN ORDER TO CATCH UP WITH THE ADVANCES IN COMPUTER/TELECOMMUNICATIONS TECHNOLOGY.

SUPERFICIALLY, ACCESS TO GOVERNMENT DOCUMENTS MAY BE VIEWED AS A CLAIM, OR PERHAPS INCREASINGLY, AS A RIGHT IN LIBERAL DEMOCRATIC SOCIETIES; THE ABILITY TO INSPECT ONE'S PERSONAL FILES HELD IN GOVERNMENT CAN BE SEEN AS SIMPLY A SUBSET OF THIS GENERAL RIGHT OF ACCESS. ALTERNATIVELY, THE ABILITY TO PROHIBIT ACCESS BY OTHERS TO ONE'S OWN INFORMATION IN GOVERNMENT DATA BANKS IS OFTEN REGARDED AS THE CONVERSE OF "FREEDOM OF INFORMATION". LAWS PROMOTING ACCESS TO GOVERNMENT RECORDS ORIGINATED OVER TWO HUNDRED YEARS AGO IN SWEDEN. THEY WERE PASSED IN AN EFFORT TO ENHANCE THE ACCOUNTABILITY OF THE STATE TO ITS CITIZENS. DATA PROTECTION LAWS, ON THE OTHER HAND, ARE A COMPARATIVELY RECENT REACTION TO WIDESPREAD FEARS ABOUT THE IMPACT OF INFORMATION TECHNOLOGY. AS COMPUTERS AND TELECOMMUNICATIONS COME TO REPRESENT THE CENTRAL NERVOUS SYSTEM OF AN INTERDEPENDENT WORLD, THE MANILA FILE FOLDER IS BEING QUICKLY

REPLACED BY THE COMPUTER PRINTOUT. THE PRINTOUT IS BEING REPLACED BY DIRECT OR REMOTE ACCESS TO GOVERNMENT DATA BANKS. BY SWEDISH LAW, FOR EXAMPLE, CITIZENS ARE NOW PERMITTED TO USE GOVERNMENT COMPUTERS FOR DIRECT ACCESS TO GOVERNMENT DATA BANKS. SINCE REMOTE ACCESS TO GOVERNMENT DATA BANKS IS POSSIBLE BEYOND ONE NATION'S BORDERS, THE ISSUE OF THE TRANSBORDER DATA FLOW OF BOTH PERSONAL AND GOVERNMENTAL INFORMATION HAS PROMPTED CALLS FOR THE COORDINATORS OF NATIONAL LAWS - IN BOTH THE DATA PROTECTION AND ACCESS TO INFORMATION FIELDS.

MY CENTRAL THEME IS THAT DESPITE THEIR DIFFERING HISTORIES, THESE TWO LEGISLATIVE FIELDS BOTH REPRESENT NO MORE THAN DIFFERENT TOOLS FOR INDIVIDUALS AND GROUPS OF INDIVIDUALS IN OUR SOCIETY TO ASSIST POWER AGAINST THE STATE AND AGAINST POWERFUL INSTITUTIONS IN THE STATE. BY SOME ESTIMATES, PRACTICALLY ONE-HALF OF CANADA'S GROSS NATIONAL PRODUCT AND MORE THAN ONE HALF OF THE EMPLOYMENT OF OUR CITIZENS IS RELATED TO THE PRODUCTION, PROCESSING, STORAGE AND USE OF INFORMATION. ¹

TO SOME, THE COMPUTER IS MERELY A NEUTRAL MACHINE; TO OTHERS, IT REPRESENTS THE "INFRASTRUCTURE OF TYRANNY". TO STILL OTHERS, LIKE MR. YONEJI MASUDA OF JAPAN'S INSTITUTE FOR THE INFORMATION SOCIETY, THE NEAR FUTURE IS KEENLY ANTICIPATED TO BE A "COMPUTOPIA", ² INFORMATION "UTILITIES" WILL PERMIT EVERYONE TO OBTAIN INFORMATION, SOLVE PROBLEMS AND CREATE UNTOLD OPPORTUNITIES, MERELY BY CONNECTING ONE'S HOME TERMINAL TO THE GOVERNMENT "UTILITY".

WHICHEVER PREDICTION PROVES TO BE TRUE, MOST DATA PROTECTION AND ACCESS TO INFORMATION ISSUES REFLECT LONG-STANDING SOCIETAL CONFLICTS OVER THE DISTRIBUTION OF POWER, BETWEEN THE STATE AND THE INDIVIDUAL, THE PRODUCER AND THE CONSUMER, AND SO FORTH. THE COMPUTER TECHNOLOGY SIMPLY SPEAKS A NEW "LANGUAGE OF POWER". ³

SISSELA BOK SUMMARIZES THIS POINT IN A COMPELLING WAY: "CONFLICTS OVER SECRECY - BETWEEN STATE AND CITIZEN... OR BETWEEN PARENT AND CHILD, OR IN JOURNALISM OR BUSINESS OR LAW - ARE CONFLICTS OVER POWER - THE POWER THAT COMES THROUGH CONTROLLING THE FLOW OF INFORMATION. TO BE ABLE TO HOLD BACK SOME INFORMATION ABOUT ONESELF OR TO CHANNEL IT AND THUS INFLUENCE HOW ONE IS SEEN BY OTHERS GIVES POWER; SO DOES THE CAPACITY TO PENETRATE SIMILAR DEFENCES AND STRATEGIES WHEN USED BY OTHERS. TRUE, POWER REQUIRES NOT ONLY KNOWLEDGE BUT THE CAPACITY TO PUT KNOWLEDGE TO USE; BUT WITHOUT THE KNOWLEDGE, THERE IS NO CHANCE TO EXERCISE POWER". ⁴

B. FADING BORDERS

THE CALL FOR DATA PROTECTION LAWS REFLECTED A WIDESPREAD CONCERN OVER INDIVIDUAL PRIVACY. PRIVACY IS AN ELUSIVE CONCEPT. SEVERAL YEARS AGO, A FEDERAL TASK FORCE ON PRIVACY AND COMPUTERS IDENTIFIED THREE DIFFERENT CONTEXTS IN WHICH THE INVASION OF PRIVACY MAY BE ASSERTED: (1) TERRITORIAL PRIVACY; (2) PRIVACY OF THE PHYSICAL PERSON AND (3) PRIVACY IN THE INFORMATION CONTEXT.⁵ ALAN WESTON DEFINED THIS NOTION OF "INFORMATIONAL PRIVACY" AS THE "CLAIM OF INDIVIDUALS, GROUPS OR INSTITUTIONS TO DETERMINE FOR THEMSELVES WHEN, HOW AND TO WHAT EXTENT INFORMATION ABOUT

THEM IS TO BE COMMUNICATED TO OTHERS".⁶

UNTIL QUITE RECENTLY, THE MAJOR SAFEGUARD OF INFORMATION PRIVACY HAD BEEN THE DIFFICULTY IN FINDING PARTICULAR INFORMATION STORED IN A VARIETY OF WAYS IN A VARIETY OF LOCATIONS. TODAY'S COMPUTERS HAVE THE SPEED AND CAPACITY TO STORE, COMBINE, RETRIEVE AND TRANSFER HUGE QUANTITIES OF DATA VERY QUICKLY AND VERY CHEAPLY.

AMONG THE O.E.C.D. COUNTRIES, 9 HAVE EXPLICIT DATA PROTECTION LAWS AT THE NATIONAL LEVEL (AUSTRIA, CANADA, DENMARK, FRANCE, GERMANY, LUXEMBOURG, NORWAY, SWEDEN AND THE U.S.A.). THE UNITED KINGDOM'S DATA PROTECTION BILL WILL BE THE TENTH SUCH LAW ON THE LIST. SOME LAWS APPLY ONLY TO PERSONAL DATA REGISTERS WHICH CONTAIN COMPUTERIZED FILES; SOME COVER MANUALLY STORED DATA AS WELL.

MOST LAWS COVER PERSONAL REGISTERS IN BOTH THE PUBLIC AND PRIVATE SECTORS; HOWEVER, SOME LAWS LIKE CANADA'S PRIVACY ACT, FOR INSTANCE, COVER ONLY PUBLIC SECTOR RECORDS. MOST SUCH LAWS PROTECT ONLY PERSONAL INFORMATION PERTAINING TO INDIVIDUALS; SOME DATA PROTECTION LAWS, HOWEVER, SUCH AS THOSE OF AUSTRIA, DENMARK, LUXEMBOURG AND NORWAY ALSO PERTAIN TO "LEGAL PERSONS" SUCH AS COMPANIES, SOCIETIES AND FOUNDATIONS. THE O.E.C.D. HAS GENERATED GUIDELINES TO HELP COORDINATE AND SUGGEST MAXIMUM DATA PROTECTION STANDARDS SO THAT VARYING NATIONAL LAWS DO NOT CREATE NON TARIFF BARRIERS TO THE FLOW OF DATA.

FREEDOM OF INFORMATION LAWS, ON THE OTHER HAND, NOW EXIST IN SOME 10 O.E.C.D. COUNTRIES, SIX OF WHICH ALSO HAVE DATA PROTECTION LAWS. JUST AS THE CONTROL OF ONE'S PERSONAL INFORMATION HAS GENERATED DATA PROTECTION LAWS, LIKEWISE THE

ACCELERATING DEMAND FOR ACCESS LAWS HAS BEEN PART OF A LARGER CONCERN OF INDIVIDUALS AND GROUPS FOR A GREATER DEGREE OF CONTROL AND PARTICIPATION IN THE GOVERNMENT DECISIONS WHICH AFFECT OUR LIVES. THE ABILITY TO PARTICIPATE IN AN AGENCY'S DECISION CONCERNING THE SITING OF A DAM OR A HAZARDOUS WASTE FACILITY OR CONCERNING A NATURAL GAS RATE INCREASE, REQUIRES FULL AND TIMELY DISCLOSURE OF INFORMATION FROM GOVERNMENT FILES. SIMILARLY, THE ABILITY TO SEE ONE'S COMPLETE WORKER'S COMPENSATION FILE OR TO PROHIBIT OTHERS FROM SEEING ONE'S PSYCHIATRIC RECORDS, IS ESSENTIAL IF AN INDIVIDUAL IS TO BE MORE THAN THE PASSIVE OBJECT OF BUREAUCRATIC WHIM. THE FIRST SET OF DECISIONS WOULD BE THE SUBJECT OF A FREEDOM OF INFORMATION LAW; THE SECOND, OF A DATA PROTECTION REGIME.

LAW REFORM IN BOTH AREAS FITS SQUARELY WITHIN A FRAMEWORK OF LAW REFORM SUCH AS LIBERALIZED STANDING RULES BEFORE COURTS AND ADMINISTRATIVE AGENCIES, COST AWARDS FOR PUBLIC INTEREST INTERVENORS AND ENHANCED "SHAREHOLDER DEMOCRACY" WITHIN CORPORATIONS. ALL OF THESE REFORMS PROMOTE CITIZEN PARTICIPATION.

HOWEVER, A GENERALIZED RIGHT TO GOVERNMENT INFORMATION CLASHES WITH AT LEAST FOUR OTHER INTERESTS, EACH OF WHICH I WILL EXAMINE IN TURN: (1) THE PRIVACY RIGHTS OF OTHER INDIVIDUALS; (2) THE STATE'S OWN INTEREST IN A CORE ZONE OF SECRECY; (3) THE CLAIMS ADVANCED BY OTHER GOVERNMENTS TO PROTECT THEIR INFORMATION IN ANOTHER GOVERNMENT'S FILES AND (4) THE RIGHT OF CORPORATIONS TO ENSURE THE SECRECY OF INFORMATION CONCERNING THEM WHICH IS FOUND IN GOVERNMENT FILES.

FIRSTLY, ALL FREEDOM OF INFORMATION LAWS CONTAIN A CLUSTER OF EXEMPTIONS THAT SEEK TO DEFEND VITAL STATE INTERESTS SUCH AS NATIONAL SECURITY, LAW ENFORCEMENT AND COHERENT POLICY FORMATION FROM UNAUTHORIZED DISTURBANCE. THE PRECISE SCOPE OF SUCH EXEMPTIONS MAY DIFFER BUT THE UNDERLYING PRINCIPLES DO NOT VARY.

SECOND, ALL FREEDOM OF INFORMATION LAWS SEEK TO PROTECT THE INDIVIDUAL'S PRIVACY FROM ALL EXCEPT THE INDIVIDUAL CONCERNED. WHEN SOMEONE REQUESTS INFORMATION CONCERNING ANOTHER, FOR EXAMPLE, FOR EPIDEMIOLOGICAL RESEARCH, A DELICATE BALANCING OF JUDGMENT IS TYPICALLY REQUIRED. THE U.S. FOIA EXEMPTS THE DISCLOSURE OF PERSONAL FILES, "THE DISCLOSURE OF WHICH WOULD CONSTITUTE A CLEARLY UNWARRANTED INVASION OF PERSONAL PRIVACY".⁷ THE NECESSARY OVERLAP BETWEEN DATA PROTECTION AND ACCESS LAWS IN THIS REGARD IS PERHAPS BEST DEMONSTRATED IN AUSTRALIA. ALTHOUGH THERE IS NO PRIVACY ACT AT THE FEDERAL LEVEL, AN INDIVIDUAL MAY SEEK ACCESS TO HIS/HER PERSONAL RECORDS UNDER THE NEW AUSTRALIAN FREEDOM OF INFORMATION ACT.⁸

THIRD, THE INFORMATION PROVIDED BY ONE GOVERNMENT TO ANOTHER IS ROUTINELY PROTECTED UNDER VARIOUS FREEDOM OF INFORMATION LAWS. FOR EXAMPLE, IN BOTH THE CANADIAN PRIVACY ACT AND THE ACCESS ACT, INFORMATION "OBTAINED IN CONFIDENCE" FROM FOREIGN GOVERNMENTS, INTERNATIONAL ORGANIZATIONS OR FROM THE GOVERNMENTS OF A PROVINCE, MUNICIPALITY OR REGIONAL DISTRICT CANNOT BE REVEALED BY A FEDERAL AGENCY.⁹ MANY DEPARTMENTS OF THE ALBERTA, BRITISH COLUMBIA AND ONTARIO GOVERNMENTS, FOR EXAMPLE, ARE SEEKING WHOLESAL PROTECTION FOR THEIR RECORDS WHICH ARE SHARED WITH OTTAWA. SOME ACCESS

LAWS LIKE THE U.S. FOIA PERMIT ACCESS TO U.S. NATIONALS AND FOREIGNERS ALIKE; OTHERS LIKE CANADA'S ACCESS ACT. RESTRICT USE TO CANADIAN CITIZENS AND LANDED IMMIGRANTS DESPITE THE TECHNOLOGICAL EASE IN RETRIEVING INFORMATION IN PUBLIC DATA BANKS FROM ABROAD. AT THE INTERNATIONAL LEVEL, NEW CHALLENGES TO NATIONAL SOVEREIGNTY ARE POSED BY THE NEW COMMUNICATION TECHNOLOGY. FOR EXAMPLE, HOW FAR SHOULD ONE GOVERNMENT OR MULTI-NATIONAL ENTERPRISE BE PERMITTED TO GO IN COLLECTING SENSITIVE DATA ON ANOTHER COUNTRY'S NATURAL RESOURCES OR ECONOMIC INFRASTRUCTURE? IS THERE A RIGHT OF ACCESS OR A PRINCIPLE OF CONSENT WHICH ALSO APPLIES TO NATION STATES?

FINALLY, BUSINESS ENTERPRISES HAVE SPECIAL CONCERNS ABOUT FREEDOM OF INFORMATION LEGISLATION. BUSINESSES, TOO, ARE CONCERNED THAT INFORMATION WHICH THEY PROVIDE TO VARIOUS GOVERNMENT AGENCIES BE ADEQUATELY SAFEGUARDED. BUT CAN A CORPORATION HAVE "PRIVACY"? SISSELA BOK ANSWERS 'NO':

"CLAIMS OF PRIVACY ARE OFTEN MADE FOR (PRACTICES OF LARGE-SCALE COLLECTIVE SECRECY SUCH AS TRADE SECRECY) AND THE METAPHORS OF PERSONAL SPACE ARE STRETCHED TO APPLY TO THEM. TO BE SURE, SUCH PRACTICES ARE AUTOMATICALLY PRIVATE IN ONE SENSE, SO LONG AS THEY ARE NOT PUBLIC. BUT THE USE OF THE LANGUAGE OF PRIVACY WITH ITS METAPHORS OF PERSONAL SPACE, SPHERES, SANCTIONS AND BOUNDARIES TO PERSONALIZE COLLECTIVE ENTERPRISES SHOULD NOT GO UNCHALLENGED. SUCH USAGE CAN BE SENTIMENTALIZED AS THE EXCESSIVE RESORT BY POETS TO THE "PATHETIC FALLACY"(IN WHICH PERSONAL FEELINGS SUCH AS GRIEF OR CRUELTY ARE ASCRIBED TO NATURE) AND CAN THUS DISTORT OUR UNDERSTANDING OF THE ROLE OF THESE ENTERPRISES", ¹⁰

THEREFORE "PRIVACY" CLAIMS ADVANCED BY CORPORATIONS ARE REALLY AN ASSERTION OF PROPERTY RIGHTS OR ASSERTIONS OF POWER VIS-A-VIS THE PUBLIC OR NOSY COMPETITORS.

ALTHOUGH CORPORATIONS ARE NOT GIVEN STATUS UNDER THE CANADIAN ACCESS ACT, THEIR PRINCIPALS OR LAWYERS MAY SEEK INFORMATION FOR THEMSELVES OR AS PART OF A CAMPAIGN OF WHAT AMERICANS HAVE TERMED "INDUSTRIAL ESPIONAGE". JUST AS WITH INDIVIDUAL PRIVACY, A DELICATE BALANCING JUDGMENT IS REQUIRED UNDER AN EXEMPTION IN THE ACCESS ACT IN ORDER TO PROTECT CONFIDENTIAL BUSINESS INFORMATION FROM WRONGFUL DISCLOSURE.¹¹ BUSINESS INFORMATION WHICH IS OTHERWISE CONFIDENTIAL MAY BE DISCLOSED "IF SUCH DISCLOSURE WOULD BE IN THE PUBLIC INTEREST AS IT RELATES TO PUBLIC HEALTH, PUBLIC SAFETY, OR PROTECTION OF THE ENVIRONMENT AND IF SUCH PUBLIC INTEREST IN DISCLOSURE CLEARLY OUTWEIGHS IN IMPORTANCE" THE BUSINESS INTEREST ASSERTED.

INTERESTINGLY, HOWEVER, GREATER RIGHTS IN THIS REGARD ARE PROVIDED TO BUSINESS INTERESTS THAN TO INDIVIDUALS IN THE CANADIAN LEGISLATION. UNDER THE ACCESS ACT, BUSINESS ENTERPRISES ARE GIVEN THE EXPLICIT RIGHT TO BE INFORMED IN WRITING OF A POSSIBLE DISCLOSURE OF THEIR INFORMATION. THEY ALSO HAVE THE RIGHT TO CONTEST SUCH DISCLOSURE ALL THE WAY TO THE COURTS IN WHAT THE AMERICANS CALL "REVERSE FOI SUITS".¹² HOWEVER, THE FEDERAL GOVERNMENT MAY RELEASE SENSITIVE PERSONAL INFORMATION TO A WIDE ARRAY OF THIRD PARTIES WITHOUT THE INDIVIDUAL'S KNOWLEDGE OR CONSENT - SUBJECT ONLY TO OVERSIGHT BY THE PRIVACY COMMISSIONER IN CERTAIN INSTANCES.¹³

THE ABILITY OF BUSINESS ENTERPRISES TO ENJOIN OTHERS FROM GAINING ACCESS TO THEIR INFORMATION FOUND IN PUBLIC SEC

DATA BANKS IS A SUBSTANTIAL COUNTERVAILLING POWER FOR OUR CORPORATE SECTOR. PROFESSOR CHRISTAN BAY, HOWEVER, WOULD EXTEND THE PRINCIPLE OF OPENNESS AND ACCOUNTABILITY WHICH FREEDOM OF INFORMATION LAWS SEEK TO FOSTER IN THE PUBLIC SECTOR TO THE PRIVATE SECTOR AS WELL. PROF. BAY ADVOCATES A RIGHT OF ACCESS TO THE INFORMATION HELD BY ALL PRIVATE COMPANIES OPERATING IN THE PUBLIC DOMAIN IN LIGHT OF THE POWER THESE INSTITUTIONS EXERCISE OVER OUR LIVES.¹⁴ HIS SUGGESTION IS CONSISTENT WITH THE INCREASING DEVELOPMENT OF PARTICIPATORY SHAREHOLDER DEMOCRACY IN THE UNITED STATES.¹⁵

C. CONCLUSION

BOTH DATA PROTECTION AND GENERAL ACCESS TO INFORMATION LAWS ARE EXAMPLES OF A TREND IN THE CANADIAN LEGAL CULTURE TOWARD THE CODIFICATION OF PROCEDURAL ENTITLEMENTS. THE CHARTER OF RIGHTS AND FREEDOMS IS ANOTHER PROMINENT EXAMPLE OF HOW AN INCREASINGLY HETEROGENEOUS SOCIETY LIKE OURS HAS BEGUN TO REQUIRE THAT CERTAIN PROCEDURAL ENTITLEMENTS BE MADE EXPLICIT. ENTITLEMENTS WHICH IN MOST CASES WERE IMPLICIT IN THE PAST HAVE NOW BECOME CONSTITUTIONAL RIGHTS. THIS TREND MAY REFLECT AN INCREASING DISTRUST OF LARGE INSTITUTIONS BY ORDINARY CITIZENS, PERHAPS FUELED BY A FEAR THAT PERSONAL PRIVACY AND SIMILAR VALUES ARE BEING ERODED BY THE COMPUTERIZED INFRASTRUCTURE OF OUR COMPLEX SOCIETY. AS THIS INFORMATION SOCIETY DEVELOPS, A COMPREHENSIVE AND INTERNATIONAL FRAMEWORK OF "INFORMATION LAW" MUST ALSO DEVELOP, WITH ALL THE BALANCING JUDGMENTS DISCUSSED ABOVE LIKEWISE MADE EXPLICIT.

IN MY VIEW, THE EMERGENCE OF THESE NEW KINDS OF PROCEDURAL RIGHTS TO INFORMATION - PERSONAL, GOVERNMENTAL AND EVEN CORPORATE - SHOULD BE UNDERSTOOD AS A CONTEMPORARY

APPLICATION OF WHAT JUSTICE FRANKFURTER SAID MANY YEARS
AGO; "THE HISTORY OF (AMERICAN) FREEDOM IS IN NO SMALL
MEASURE THE HISTORY OF PROCEDURE",¹⁶

- THANK YOU -

END NOTES

1. THIS FIGURE IS QUOTED FROM R. GRANT HAMMOND, "QUANTUM PHYSICS, ECONOMETRIC MODELS AND PROPERTY RIGHTS TO INFORMATION" (1981) 27 MCGILL L.J. 47 AT 48.
2. Y. MASUDA, THE INFORMATION SOCIETY AS POST-INDUSTRIAL SOCIETY (TOKYO: INSTITUTE FOR THE INFORMATION SOCIETY 1980) AT 114, 146.
3. H. BURKERT, "A FUNCTIONAL EXPLANATION OF DATA PROTECTION LAWS" (1982) COMPUTER L.J. 169.
4. S. BOK, SECRETS (NEW YORK: PANTHEON BOOKS, 1982), P. 19.
5. CANADA, DEPARTMENT OF COMMUNICATIONS AND DEPARTMENT OF JUSTICE, PRIVACY AND COMPUTERS (OTTAWA: INFORMATION CANADA, 1971) AT P. 13-14.
6. ALAN F. WESTIN, PRIVACY AND FREEDOM (NEW YORK - ATHENUM PRESS, 1967) AT P. 7.
7. USCA S.552 (B) (6).
8. S. 41 OF THE AUSTRALIAN FREEDOM OF INFORMATION ACT EXEMPTS DOCUMENTS THE DISCLOSURE OF WHICH WOULD INVOLVE "THE UNREASONABLE DISCLOSURE OF PERSONAL INFORMATION". HOWEVER, SECTION 41(2) STATES THAT THIS DOES NOT AFFECT AN INDIVIDUAL'S REQUEST FOR ACCESS TO ONE'S OWN INFORMATION. SECTION 45 ALSO EXEMPTS THE DISCLOSURE OF INFORMATION THAT "WOULD CONSTITUTE A

BREACH OF CONFIDENCE', WHICH HAS ALSO BEEN INTERPRETED TO SAFEGUARD PERSONAL PRIVACY. RECENTLY, THE AUSTRALIAN LAW REFORM COMMISSION RECOMMENDED THE PASSAGE OF A PRIVACY ACT TO CLARIFY THE SCOPE OF INFORMATIONAL PRIVACY AND TO EXTEND THE RIGHT OF ACCESS TO THE PRIVATE SECTOR, STARTING WITH THE AUSTRALIAN COMMONWEALTH TERRITORY.

9. S. 19 PRIVACY ACT; S. 13 ACCESS TO INFORMATION ACT.
10. S. BOK, OP. CIT, SUPRA NOTE 4, AT P. 13-14.
11. SEE S. 20 (6) ACCESS TO INFORMATION ACT.
12. THE FIRST CASE DECIDED UNDER THE ACCESS TO INFORMATION ACT RAISED JUST THIS KIND OF ISSUE: MAISLIN INDUSTRIES LTD. V. MINISTER OF INDUSTRY, TRADE AND COMMERCE ET AL (FEDERAL COURT, TRIAL DIVISION PER JEROME, A.C.J. MAY 9, 1984).
13. SECTION 8(2) OF THE PRIVACY ACT SETS OUT 13 WIDE CATEGORIES IN WHICH THE DISCLOSURE OF PERSONAL INFORMATION TO THIRD PARTIES IS AUTHORIZED.
14. C. BAY - "COMMENT", IN J.D. MCCAMUS, FREEDOM OF INFORMATION: CANADIAN PROSPECTIVES (TORONTO: BUTTERWORTHS, 1981), P. 23
15. SEE DISCUSSION IN JOHN NAISBITT, MEGATRENDS (NEW YORK: WARNER BOOKS, 1984), P. 197.
16. MALINSKI V STATE OF NEW YORK (1945), 324, U.S. 401, 411, (FRANKFURTER, J.)

DOCUMENT: 870-123/011

Traduction du Secrétariat

CONFÉRENCE INTERPROVINCIALE SUR LA PROTECTION DES
RENSEIGNEMENTS PERSONNELS: MESURES POUR 1984 (COLLOQUE)

L'accès à l'information et les limites de la vie privée:
À la recherche d'un équilibre

T. Murray Rankin
Faculté de droit
Université de Victoria

Toronto (Ontario)
Les 23 et 24 mai 1984

A. INTRODUCTION

HISTORIQUEMENT, LES ORIGINES DES LOIS RELATIVES À LA PROTECTION DES DONNÉES ET DE CELLES PORTANT SUR LA LIBERTÉ D'INFORMATION REMONTENT À DES SOURCES DIFFÉRENTES. CES LOIS ONT EN EFFET VU LE JOUR AU FIL DE L'HISTOIRE EUROPÉENNE EN RÉACTION À DES PROBLÈMES PARTICULIERS. À L'HEURE ACTUELLE, CEPENDANT, BEAUCOUP CONFONDENT CES DEUX NOTIONS JURIDIQUES DISTINCTES. JE SOUTIENS QUE CET AMALGAMME DÉCOULE DES RÉCENTES RÉALISATIONS TECHNOLOGIQUES QUI CONTRIBUENT À CRÉER NOTRE "SOCIÉTÉ D'INFORMATION" GLOBALE. LE CHEVAUCHEMENT DE CES DEUX RÉGIMES LÉGISLATIFS EST PEUT-ÊTRE LE SIGNE AVANT-COUREUR DE LA CRÉATION D'UN "DROIT EXHAUSTIF DE L'INFORMATION" À MESURE QUE NOS RÈGLES JURIDIQUES ÉVOLUERONT POUR S'ADAPTER AUX PROGRÈS RÉALISÉS DANS LE DOMAINE DES TECHNIQUES DE TÉLÉCOMMUNICATIONS ET D'INFORMATIQUE.

AU PREMIER ABORD, L'ACCÈS AUX DOCUMENTS GOUVERNEMENTAUX PEUT ÊTRE CONSIDÉRÉ COMME ÉTANT UNE REVENDICATION JUSTIFIABLE OU, DE PLUS EN PLUS, DANS DES SOCIÉTÉS DÉMOCRATIQUES LIBÉRALES, EN TANT QUE DROIT. LA POSSIBILITÉ D'EXAMINER LES DOSSIERS QUE DÉTIENNENT LES GOUVERNEMENTS AU SUJET D'UNE PERSONNE PEUT ÊTRE CONSIDÉRÉE COMME UN SIMPLE EFFET SECONDAIRE DE CE DROIT D'ACCÈS GÉNÉRAL. PAR AILLEURS, LA POSSIBILITÉ D'INTERDIRE À AUTRUI L'ACCÈS AUX RENSEIGNEMENTS QUE RENFERMENT LES BANQUES DE DONNÉES GOUVERNEMENTALES AU SUJET D'UNE PERSONNE EST SOUVENT CONSIDÉRÉE COMME LE CONTRAIRE MÊME DE LA "LIBERTÉ D'INFORMATION". LES LOIS PRÉCONISANT L'ACCÈS AUX DOSSIERS GOUVERNEMENTAUX ONT VU LE JOUR IL Y A PLUS DE DEUX SIÈCLES EN SUÈDE. LEUR ADOPTION VISAIT À ACCROÎTRE LA RESPONSABILITÉ DE L'ÉTAT À L'ENDROIT DE SES CITOYENS. LES LOIS RELATIVES À LA PROTECTION DES DONNÉES CONSTITUENT EN REVANCHE UNE RÉACTION CONSIDÉRABLEMENT PLUS RÉCENTE AUX CRAINTES GRANDISSANTES QUE SUSCITENT LES RÉPERCUSSIONS ÉVENTUELLES DE LA TECHNOLOGIE DE L'INFORMATION. À MESURE QUE LES ORDINATEURS ET LES TÉLÉCOMMUNICATIONS SE CONSTITUENT EN SYSTÈME NERVEUX CENTRAL D'UN MONDE INTERDÉPENDANT, LE SIMPLE CLASSEUR MANUEL CÈDE RAPIDEMENT LA PLACE AU RELEVÉ D'ORDINATEUR, LEQUEL EST EN VOIE D'ÊTRE REMPLACÉ PAR L'ACCÈS DIRECT OU ÉLOIGNÉ AUX BANQUES DE DONNÉES GOUVERNEMENTALES. EN SUÈDE, PAR EXEMPLE, LES CITOYENS SONT MAINTENANT AUTORISÉS PAR LA LOI À UTILISER DES ORDINATEURS GOUVERNEMENTAUX POUR AVOIR DIRECTEMENT ACCÈS AUX BANQUES DE DONNÉES GOUVERNEMENTALES. ÉTANT DONNÉ QUE L'ACCÈS À DISTANCE À CES BANQUES EST POSSIBLE AU DELÀ DES FRONTIÈRES D'UN PAYS DONNÉ, LA QUESTION DE LA CIRCULATION OUTRE-FRONTIÈRE DE DONNÉES TOUCHANT DES RENSEIGNEMENTS TANT GOUVERNEMENTAUX QUE PERSONNELS FAVORISE LE RECOURS AUX COORDONNATEURS DES LOIS NATIONALES, AUSSI BIEN DANS LE DOMAINE DE LA PROTECTION DES DONNÉES QUE DANS CELUI DE L'ACCÈS À L'INFORMATION.

CE QUE JE SOUTIENS PRINCIPALEMENT, C'EST QU'EN DÉPIT DE LA DIFFÉRENCE DE LEUR HISTORIQUE, CES DEUX DOMAINES LÉGISLATIFS REPRÉSENTENT SIMPLEMENT DES OUTILS DIFFÉRENTS MIS À LA DISPOSITION DES PARTICULIERS ET DES GROUPES DANS NOTRE SOCIÉTÉ POUR ACQUÉRIR DU POUVOIR FACE À L'ÉTAT ET À SES PUISSANTES INSTITUTIONS. D'APRÈS CERTAINS CALCULS, PRATIQUEMENT LA MOITIÉ DU PRODUIT NATIONAL BRUT DU CANADA ET PLUS DE LA MOITIÉ DE L'EMPLOI DE NOS CITOYENS SONT LIÉES À LA PRODUCTION, AU TRAITEMENT, À L'ENTREPOSAGE ET À L'UTILISATION DE L'INFORMATION¹.

AUX YEUX DE CERTAINS, L'ORDINATEUR EST UNE SIMPLE MACHINE NEUTRE; POUR D'AUTRES, EN REVANCHE, IL REPRÉSENTE "L'INFRASTRUCTURE DE LA TYRANNIE". POUR D'AUTRES ENCORE, COMME M. YONEJI MASUADA, DE L'INSTITUTE FOR THE INFORMATION SOCIETY (JAPON), L'AVENIR PRÉVISIBLE SERA SANS DOUTE MARQUÉ PAR "LE RÈGNE DE L'ORDINATEUR" (COMPUTOPIA)². DES "SERVICES PUBLICS" D'INFORMATION PERMETTRONT À CHACUN D'OBTENIR DES RENSEIGNEMENTS, RÉSOUDRONT DES PROBLÈMES ET CRÉERONT DES PERSPECTIVES INIMAGINABLES, PAR LE SIMPLE FAIT DE RACCORDER LE TERMINAL PERSONNEL D'UN PARTICULIER AUX "SERVICES PUBLICS" DU GOUVERNEMENT.

QUELLE QUE SOIT LA PRÉDICTION QUI SE RÉALISERA, LA PLUPART DES QUESTIONS RELATIVES À LA PROTECTION DES DONNÉES ET À L'ACCÈS À L'INFORMATION TRADUISENT DES CONFLITS DE LONGUE DATE AU SEIN DE LA SOCIÉTÉ AU SUJET DE LA RÉPARTITION DU POUVOIR, ENTRE L'ÉTAT ET LE PARTICULIER, ENTRE LE PRODUCTEUR ET LE CONSOMMATEUR, ET AINSI DE SUITE. EN FAIT, LA TECHNOLOGIE DE L'ORDINATEUR PARLE UN NOUVEAU "LANGAGE DU POUVOIR"³.

SISSELA BOK RÉSUME TRÈS BIEN LA QUESTION:

(TRADUCTION NON OFFICIELLE)

"LES DIFFÉRENDS QUI PORTENT SUR LE SECRET - QUE CE SOIT ENTRE L'ÉTAT ET LE CITOYEN... OU ENTRE LE PARENT ET L'ENFANT, OU ENCORE DANS LE MONDE DU JOURNALISME, DES AFFAIRES OU DU DROIT - SONT DES LUTTES POUR LE POUVOIR, LE POUVOIR QUI ÉMANÉ DU CONTRÔLE DE L'INFORMATION. LE FAIT D'ÊTRE CAPABLE DE GARDER SECRETS CERTAINS RENSEIGNEMENTS À SON PROPRE SUJET OU DE LES CANALISER ET D'INFLUENCER AINSI LA PERCEPTION QUE LES AUTRES ONT DE SOI DONNE DU POUVOIR; TOUT COMME LE FAIT D'ÊTRE CAPABLE DE PERCER DES DÉFENSES ET DES STRATÉGIES SEMBLABLES LORSQU'ELLES SONT UTILISÉES PAR D'AUTRES. CERTES, LE POUVOIR NÉCESSITE NON SEULEMENT DES CONNAISSANCES MAIS ÉGALEMENT LA CAPACITÉ D'UTILISER CES CONNAISSANCES; MAIS IL N'EN RESTE PAS MOINS QUE, SANS LA CONNAISSANCE, IL N'Y A AUCUNE POSSIBILITÉ D'EXERCER LE POUVOIR"⁴.

B. L'EFFACEMENT DES FRONTIÈRES

LES REVENDICATIONS VISANT L'ADOPTION DE LOIS SUR LA PROTECTION DES DONNÉES TRADUISENT L'AMPLEUR DES INQUIÉTUDES CONCERNANT LA VIE PRIVÉE DES PARTICULIERS. LA NOTION DE VIE PRIVÉE EST DIFFICILE À CERNER. IL Y A QUELQUES ANNÉES, UN GROUPE D'ÉTUDE FÉDÉRAL SUR L'ORDINATEUR ET LA VIE PRIVÉE RELEVAIT TROIS SPHÈRES DIFFÉRENTES SE PRÊTANT À L'EXERCICE DU DROIT À LA VIE PRIVÉE : 1) LA VIE PRIVÉE AU SENS SPATIAL; 2) LA VIE PRIVÉE DE LA PERSONNE ET 3) LA VIE PRIVÉE DANS LE CONTEXTE DE L'INFORMATION⁵. POUR ALAN WESTON, LA NOTION DE VIE PRIVÉE EN MATIÈRE D'INFORMATION SERAIT LE DROIT DES PARTICULIERS, DES GROUPES OU DES INSTITUTIONS DE DÉTERMINER PERSONNELLEMENT QUAND, COMMENT ET DANS QUELLE MESURE LES DONNÉES LES CONCERNANT PEUVENT ÊTRE COMMUNIQUÉES À D'AUTRES⁶.

JUSQU'À TOUT RÉCEMMENT, LA PRINCIPALE GARANTIE DU RESPECT DU CARACTÈRE PRIVÉ DE L'INFORMATION TENAIT AU FAIT QU'IL ÉTAIT DIFFICILE DE TROUVER DES RENSEIGNEMENTS PRÉCIS CONSERVÉS DE MULTIPLES MANIÈRES À DE MULTIPLES ENDROITS. OR, LES ORDINATEURS D'AUJOURD'HUI SONT DOTÉS DE LA VITESSE ET DE LA CAPACITÉ NÉCESSAIRES POUR ENTREPOSER, COMBINER, RETIRER ET TRANSFÉRER D'IMMENSES VOLUMES DE DONNÉES, ET CE, TRÈS RAPIDEMENT ET À TRÈS BON MARCHÉ.

PARMI LES PAYS DE L'OCDE, NEUF DISPOSENT DE LOIS EXPLICITES SUR LA PROTECTION DES DONNÉES À L'ÉCHELLE NATIONALE (L'AUTRICHE, LE CANADA, LE DANEMARK, LA FRANCE, L'ALLEMAGNE, LE LUXEMBOURG, LA NORVÈGE, LA SUÈDE ET LES ÉTATS-UNIS). LA LOI SUR LA PROTECTION DES DONNÉES DU ROYAUME-UNI S'INSCRIRA DONC EN DIXIÈME PLACE SUR LA LISTE. CERTAINES LOIS NE VISENT QUE LES RÉPERTOIRES DE DONNÉES PERSONNELLES QUE RENFERMENT DES DOSSIERS INFORMATISÉS, TANDIS QUE D'AUTRES VISENT ÉGALEMENT LES DONNÉES CONSERVÉES EN VERTU D'UN SYSTÈME MANUEL.

LA PLUPART DES LOIS VISENT LES RÉPERTOIRES PERSONNELS DANS LES SECTEURS PUBLIC ET PRIVÉ; CEPENDANT, CERTAINES, COMME LA LOI CANADIENNE SUR LA PROTECTION DE LA VIE PRIVÉE, NE VISENT QUE LES DOSSIERS DU SECTEUR PUBLIC. LA PLUPART DE CES LOIS NE PROTÈGENT QUE LES DONNÉES PERSONNELLES AYANT TRAIT À DES PARTICULIERS; CEPENDANT, CERTAINES LOIS SUR LA PROTECTION DES DONNÉES, COMME CELLES DE L'AUTRICHE, DU DANEMARK, DU LUXEMBOURG ET DE LA NORVÈGE, VISENT ÉGALEMENT LES "PERSONNES LÉGALES" COMME LES COMPAGNIES, LES SOCIÉTÉS ET LES FONDATIONS. L'OCDE A CONÇU DES LIGNES DIRECTIVES POUR AIDER À COORDONNER ET À PROPOSER DES NORMES MAXIMALES DE PROTECTION DES DONNÉES DE SORTE QUE LES DIFFÉRENTES LOIS NATIONALES NE CRÉENT PAS DE BARRIÈRE NON TARIFAIRES À LA LIBRE CIRCULATION DES DONNÉES.

PAR AILLEURS, DES LOIS SUR LA LIBERTÉ D'INFORMATION EXISTENT ACTUELLEMENT DANS QUELQUE DIX PAYS DE L'OCDE, DONT SIX DISPOSENT ÉGALEMENT DE LOIS SUR LA PROTECTION DES DONNÉES. TOUT COMME LE CONTRÔLE DES DONNÉES PERSONNELLES A SUSCITÉ L'ADOPTION DE LOIS SUR LA PROTECTION DES DONNÉES, LA DEMANDE CROISSANTE DE LOIS PORTANT SUR L'ACCÈS À L'INFORMATION S'INSCRIT DANS UN PLUS LARGE COURANT DE PARTICULIERS ET DE GROUPES QUI RÉCLAMENT DAVANTAGE DE CONTRÔLE ET DE PARTICIPATION EN CE QUI A TRAIT AUX DÉCISIONS GOUVERNEMENTALES QUI INFLUENT SUR LEUR VIE. POUR QU'UNE PERSONNE PUISSE PARTICIPER À LA PRISE DE DÉCISIONS D'UN ORGANISME AU SUJET DE L'EMPLACEMENT D'UN BARRAGE OU D'UNE INSTALLATION DE DÉCHETS DANGEREUX OU ENCORE DE L'AUGMENTATION DU PRIX DU GAZ NATUREL, IL FAUT D'ABORD QUE LES DONNÉES CONTENUES DANS LES DOSSIERS GOUVERNEMENTAUX SOIENT PLEINEMENT DIVULGUÉS AU MOMENT VOULU. DE MÊME, IL EST ESSENTIEL QU'UNE PERSONNE PUISSE CONSULTER LA TOTALITÉ DU DOSSIER QUI LA CONCERNE EN MATIÈRE D'INDEMNISATION DES TRAVAILLEURS OU ENCORE QU'ELLE PUISSE INTERDIRE À D'AUTRES L'ACCÈS À SON DOSSIER PSYCHIATRIQUE, SINON LE PARTICULIER NE SERAIT GUÈRE PLUS QU'UN JOUET PASSIF À LA MERCI DES CAPRICES DE LA BUREAUCRATIE. LE PREMIER ENSEMBLE DE DÉCISIONS RELÈVERAIT D'UNE LOI SUR LA LIBERTÉ D'INFORMATION; LE SECOND, D'UN RÉGIME VISANT LA PROTECTION DES DONNÉES.

DANS LES DEUX DOMAINES, LA RÉFORME DU DROIT S'INSCRIT ÉTROITEMENT DANS LE CADRE D'UNE RÉFORME JURIDIQUE TELLE QUE LA LIBÉRALISATION DES RÈGLEMENTS DES TRIBUNAUX ET DES ORGANISMES ADMINISTRATIFS, L'OCTROI D'UNE INDEMNISATION MONÉTAIRE À DES INTERVENANTS DÉFENSEURS DE L'INTÉRÊT PUBLIC ET LA PERÇÉE DE LA "DÉMOCRATIE DE L'ACTIONNAIRE" AU SEIN DES SOCIÉTÉS. TOUTES CES RÉFORMES PRÉCONISENT LA PARTICIPATION DU CITOYEN.

CEPENDANT, UN DROIT GÉNÉRALISÉ À L'INFORMATION GOUVERNEMENTALE ENTRE EN CONTRADICTION AVEC AU MOINS QUATRE AUTRES INTÉRÊTS, QUE JE VAIS MAINTENANT ÉTUDIER À TOUR DE RÔLE: 1) LES DROITS À LA VIE PRIVÉE DES AUTRES PARTICULIERS; 2) L'INTÉRÊT PROPRE DE L'ÉTAT DANS UN SECTEUR DONNÉ DE RENSEIGNEMENTS SECRETS; 3) LES DEMANDES FAITES PAR D'AUTRES GOUVERNEMENTS AFIN DE PROTÉGER LES RENSEIGNEMENTS QUE RËNFERMENT À LEUR SUJET LES DOSSIERS D'UN GOUVERNEMENT ET 4) LE DROIT DES SOCIÉTÉS DE FAIRE EN SORTE QUE RESTENT SECRETS LES RENSEIGNEMENTS QUI LES CONCERNENT DANS LES DOSSIERS GOUVERNEMENTAUX.

PREMIÈREMENT, TOUTES LES LOIS SUR LA LIBERTÉ DE L'INFORMATION RËNFERMENT DE NOMBREUSES EXEMPTIONS QUI VISENT À PROTÉGER DE TOUTE PERTURBATION NON AUTORISÉE DES INTÉRÊTS D'ÉTAT VITAUX COMME LA SÉCURITÉ NATIONALE, L'APPLICATION DE LA LOI ET L'ÉLABORATION DE POLITIQUES COHÉRENTES. LA PORTÉE PRÉCISE DE PAREILLES EXEMPTIONS PEUT VARIER MAIS LES PRINCIPES SOUS-JACENTS RESTENT LES MÊMES.

DEUXIÈMEMENT, TOUTES LES LOIS SUR LA LIBERTÉ DE L'INFORMATION VISENT LA PROTECTION DE LA VIE PRIVÉE DU PARTICULIER PAR RAPPORT À TOUTES LES PARTIES SAUF LA PERSONNE CONCERNÉE. LORSQUE QUELQU'UN A BESOIN D'INFORMATION AU SUJET DE QUELQU'UN D'AUTRE, PAR EXEMPLE DANS LE CADRE D'UNE RECHERCHE ÉPIDÉMIOLOGIQUE, LE JUGEMENT RENDU DOIT ÊTRE PARTICULIÈREMENT NUANCÉ. PAR EXEMPLE, LA LOI AMÉRICAINE "FOIA" FAIT EXCEPTION DE LA DIVULGATION DE DOSSIERS PERSONNELS DONT LA DIVULGATION CONSTITUERAIT UNE INTRUSION NETTEMENT INJUSTIFIÉE DANS LA VIE PRIVÉE D'UNE PERSONNE⁷. C'EST SANS DOUTE EN AUSTRALIE QU'ON TROUVE LE MEILLEUR EXEMPLE DU CHEVAUCHEMENT NÉCESSAIRE À CET ÉGARD ENTRE LES LOIS SUR LA PROTECTION DES DONNÉES ET CELLES SUR L'ACCÈS À L'INFORMATION. MÊME S'IL N'EXISTE PAS DE LOI SUR LA VIE PRIVÉE AU PALIER FÉDÉRAL, UN PARTICULIER PEUT TENTER D'AVOIR ACCÈS AUX DOSSIERS LE CONCERNANT EN VERTU DE LA NOUVELLE LOI AUSTRALIENNE SUR LA LIBERTÉ D'INFORMATION⁸.

TROISIÈMEMENT, LES RENSEIGNEMENTS FOURNIS PAR UN GOUVERNEMENT À UN AUTRE SONT HABITUELLEMENT PROTÉGÉS EN VERTU DE DIVERSES LOIS SUR LA LIBERTÉ D'INFORMATION. PAR EXEMPLE, DANS LES LOIS CANADIENNES SUR L'ACCÈS À L'INFORMATION D'UNE PART ET LA PROTECTION DES RENSEIGNEMENTS PERSONNELS D'AUTRE PART, UNE INSTITUTION FÉDÉRALE EST TENUE DE REFUSER LA COMMUNICATION DE RENSEIGNEMENTS "OBTENUS À TITRE CONFIDENTIEL" DE GOUVERNEMENTS ÉTRANGERS, D'ORGANISATIONS INTERNATIONALES OU DES GOUVERNEMENTS DES PROVINCES, DES ADMINISTRATIONS MUNICIPALES OU RÉGIONALES⁹. PAR EXEMPLE, PLUSIEURS MINISTÈRES DES GOUVERNEMENTS DE L'ALBERTA, DE LA COLOMBIE-BRITANNIQUE ET DE L'ONTARIO CHERCHENT À PROTÉGER INTÉGRALEMENT LES DOSSIERS QU'ILS PARTAGENT AVEC OTTAWA. CERTAINES LOIS SUR L'ACCÈS À L'INFORMATION, COMME LA "FOIA" AUX ÉTATS-UNIS, PERMETTENT L'ACCÈS AUSSI BIEN AUX RESSORTISSANTS AMÉRICAINS QU'AUX ÉTRANGERS; ALORS QUE D'AUTRES, COMME LA LOI CANADIENNE SUR L'ACCÈS À L'INFORMATION, RESTREIGNENT L'USAGE AUX CITOYENS CANADIENS ET AUX IMMIGRANTS REÇUS EN DÉPIT DU FAIT QUE LES MOYENS TECHNIQUES ACTUELS PERMETTENT FACILEMENT À DES ÉTRANGERS DE RETIRER DES RENSEIGNEMENTS DE BANQUES DE DONNÉES PUBLIQUES. AU NIVEAU INTERNATIONAL, LA NOUVELLE TECHNIQUE DES COMMUNICATIONS POSE DE NOUVEAUX DÉFIS À LA SOUVERAINETÉ NATIONALE. PAR EXEMPLE, JUSQU'OU DOIVENT ALLER UN GOUVERNEMENT OU UNE MULTINATIONALE LORSQU'ILS RECUEILLENENT DES DONNÉES DÉLICATES SUR LES RESSOURCES NATURELLES OU L'INFRASTRUCTURE ÉCONOMIQUE D'UN AUTRE PAYS? EXISTE-T-IL UN DROIT D'ACCÈS OU UN PRINCIPE DE CONSENTEMENT QUI S'APPLIQUERAIT ÉGALEMENT AUX ÉTATS NATIONS?

ENFIN, LES ENTREPRISES COMMERCIALES NOURRISSENT DES INQUIÉTUDES PARTICULIÈRES AU SUJET DES LOIS SUR LA LIBERTÉ D'INFORMATION. EN EFFET, LES ENTREPRISES TIENNENT ELLES AUSSI À CE QUE LES RENSEIGNEMENTS QU'ELLES FOURNISSENT AUX DIVERS ORGANISMES GOUVERNEMENTAUX SOIENT ADÉQUATEMENT PROTÉGÉS. TOUTEFOIS, UNE SOCIÉTÉ PEUT-ELLE AVOIR UNE "VIE PRIVÉE"? "NON", RÉPOND SISSELA BOK:

(TRADUCTION NON OFFICIELLE)

"ON INVOQUE SOUVENT LE DROIT AU RESPECT DE LA VIE PRIVÉE DANS LE CAS DE PRATIQUES FAVORISANT LE RECOURS AU SECRET COLLECTIF SUR UNE LARGE ÉCHELLE (COMME LE SECRET COMMERCIAL) ET ON S'ÉVERTUE À Y APPLIQUER LE PRINCIPE DE LA VIE PRIVÉE AU SENS SPATIAL. CERTES, LES PRATIQUES DE CE GENRE SONT AUTOMATIQUEMENT PRIVÉES DANS UN SENS, C'EST-À-DIRE DANS LA MESURE OÙ ELLES NE SONT PAS PUBLIQUES. CEPENDANT, LE RECOURS À LA NOTION DE VIE PRIVÉE AVEC SES MÉTAPHORES D'ESPACE PERSONNEL, DE SPHÈRES, DE SANCTIONS ET DE FRONTIÈRES AFIN DE PERSONNALISER DES ENTREPRISES COLLECTIVES NE DEVRAIT PAS ÉCHAPPER À LA CONTESTATION. EN EFFET, LE RECOURS À CE GENRE DE VOCABULAIRE RESSEMBLE AUX EXCÈS POÉTIQUES QUI TOMBENT DANS "L'ANIMISME" (PROCESSUS PAR LEQUEL DES SENTIMENTS HUMAINS COMME LE CHAGRIN OU LA CRUAUTÉ SONT ATTRIBUÉS À LA NATURE) ET PEUT AINSI FAUSSER NOTRE PERCEPTION DU RÔLE DE CES ENTREPRISES¹⁰".

PAR CONSÉQUENT, LES DEMANDES DE "RESPECT DE LA VIE PRIVÉE" FAITES PAR DES SOCIÉTÉS SONT EN FAIT UNE AFFIRMATION DE LEUR DROIT DE PROPRIÉTÉ OU DE LEUR POUVOIR PAR RAPPORT AU PUBLIC OU À DES CONCURRENTS TROP CURIEUX.

MÊME SI LES SOCIÉTÉS N'ONT PAS DE STATUT EN VERTU DE LA LOI CANADIENNE SUR L'ACCÈS À L'INFORMATION, LEURS DIRIGEANTS OU LEURS AVOCATS PEUVENT TENTER D'OBTENIR DES RENSEIGNEMENTS POUR EUX-MÊMES OU DANS LE CADRE DE CE QUE LES AMÉRICAINS APPELLENT "L'ESPIONNAGE INDUSTRIEL". TOUT COMME DANS LE CAS DU RESPECT DE LA VIE PRIVÉE DES PARTICULIERS, IL IMPORTE DE FAIRE PREUVE D'UN JUGEMENT TRÈS NUANCÉ EN VERTU D'UNE EXEMPTION PRÉVUE DANS LA LOI SUR L'ACCÈS À L'INFORMATION AFIN DE PROTÉGER DES DONNÉES COMMERCIALES CONFIDENTIELLES D'UNE DIVULGATION NON FONDÉE¹¹. DES RENSEIGNEMENTS D'AFFAIRES QUI SONT PAR AILLEURS CONFIDENTIELS PEUVENT ÊTRE COMMUNIQUÉS "POUR DES RAISONS D'INTÉRÊT PUBLIC CONCERNANT LA SANTÉ ET LA SÉCURITÉ PUBLIQUES AINSI QUE LA PROTECTION DE L'ENVIRONNEMENT; LES RAISONS D'INTÉRÊT PUBLIC DOIVENT DE PLUS JUSTIFIER NETTEMENT LES CONSÉQUENCES ÉVENTUELLES DE LA COMMUNICATION" SUR LES INTÉRÊTS COMMERCIAUX EN JEU.

IL EST CEPENDANT INTÉRESSANT DE NOTER QUE LA LOI CANADIENNE ACCORDE PLUS DE DROITS À CET ÉGARD AUX ENTREPRISES COMMERCIALES QU'AUX PARTICULIERS. EN VERTU DE LA LOI SUR L'ACCÈS À L'INFORMATION, LES ENTREPRISES COMMERCIALES ONT LE DROIT EXPLICITE D'ÊTRE INFORMÉES PAR ÉCRIT DE LA DIVULGATION ÉVENTUELLE DE LEURS RENSEIGNEMENTS. ELLES ONT ÉGALEMENT LE DROIT DE CONTESTER CETTE DIVULGATION EN UTILISANT PLEINEMENT LE PROCESSUS DES TRIBUNAUX DANS DES POURSUITES QUE LES AMÉRICAINS APPELLENT DES "REVERSE FOI SUITS"¹². CEPENDANT, LE GOUVERNEMENT FÉDÉRAL PEUT COMMUNIQUER DES RENSEIGNEMENTS À CARACTÈRE DÉLICAT SUR UNE PERSONNE À UNE VASTE GAMME DE TIERCES PARTIES SANS QUE LE PARTICULIER Y CONSENTE OU EN SOIT INFORMÉ, ET CETTE DÉCISION NE PEUT ÊTRE RÉÉVALUÉE QUE PAR LE COMMISSAIRE À LA PROTECTION DE LA VIE PRIVÉE DANS CERTAINS CAS¹³.

LE FAIT QUE LES ENTREPRISES COMMERCIALES PUISSENT INTERDIRE À D'AUTRES L'ACCÈS AUX RENSEIGNEMENTS QU'ELLES ONT COMMUNIQUÉS AUX BANQUES DE DONNÉES DU SECTEUR PUBLIC CONSTITUE UN POUVOIR D'OPPOSITION CONSIDÉRABLE POUR NOTRE SECTEUR COMMERCIAL. LE PROFESSEUR CHRISTIAN BAY, CEPENDANT, ÉTENDRAIT AU SECTEUR PRIVÉ LE PRINCIPE D'OUVERTURE ET DE RESPONSABILITÉ QUE LES LOIS SUR LA LIBERTÉ D'INFORMATION TENTENT DE FAVORISER DANS LE SECTEUR PUBLIC. M. BAY PRÉCONISE UN DROIT D'ACCÈS À L'INFORMATION DÉTENUE PAR TOUTES LES SOCIÉTÉS PRIVÉES OEUVRANT DANS LE DOMAINE PUBLIC EN FONCTION DU POUVOIR QUE CES INSTITUTIONS EXERCENT DANS NOS VIES¹⁴. SA PROPOSITION EST CONFORME AU DÉVELOPPEMENT CROISSANT DE LA PARTICIPATION EN VERTU DE LA DÉMOCRATIE DE L'ACTIONNAIRE AUX ÉTATS-UNIS¹⁵.

C. CONCLUSION

LES LOIS SUR LA PROTECTION DES DONNÉES ET LES LOIS GÉNÉRALES SUR L'ACCÈS À L'INFORMATION TRADUISENT UNE TENDANCE, DANS LA CULTURE JURIDIQUE CANADIENNE, VERS LA CODIFICATION DE DROITS DE PROCÉDURE. LA CHARTE DES DROITS ET LIBERTÉS CONSTITUE UN AUTRE EXEMPLE NOTABLE DE LA FAÇON DONT UNE SOCIÉTÉ DE PLUS EN PLUS HÉTÉROGÈNE COMME LA NÔTRE A COMMENCÉ À EXIGER QUE CERTAINS DROITS EN MATIÈRE DE PROCÉDURE SOIENT RENDUS PLUS EXPLICITES. CERTAINS TITRES QUI, DANS LA PLUPART DES CAS, ÉTAIENT IMPLICITES PAR LE PASSÉ SONT MAINTENANT DEVENUS DES DROITS CONSTITUTIONNELS. CETTE TENDANCE PEUT TRADUIRE UNE MÉFIANCE GRANDISSANTE DES CITOYENS ORDINAIRES À L'ENDROIT DES GRANDES INSTITUTIONS, MÉFIANCE QUI EST PEUT-ÊTRE ALIMENTÉE PAR LA PEUR QUE LE RESPECT DE LA VIE PRIVÉE DES PERSONNES ET DES VALEURS SIMILAIRES SUBISSENT UNE ÉROSION GRADUELLE SOUS LA PRESSION DE L'INFRASTRUCTURE INFORMATISÉE DE NOTRE SOCIÉTÉ COMPLEXE. À MESURE QUE SE DÉVELOPPER LA SOCIÉTÉ DE L'INFORMATION, IL SERA ESSENTIEL D'ÉDIFIER ÉGALEMENT UN CADRE INTERNATIONAL ET EXHAUSTIF POUR LE "DROIT DE L'INFORMATION", EN RENDANT ÉGALEMENT EXPLICITES TOUS LES JUGEMENTS NUANCÉS DONT IL A ÉTÉ QUESTION CI-DESSUS.

À MON AVIS, L'ÉMERGENCE DE CES NOUVEAUX TYPES DE DROIT PROCÉDURIERS À L'INFORMATION (D'ORDRE PERSONNEL, GOUVERNEMENTAL, VOIRE COMMERCIAL) DEVRAIT ÊTRE CONSIDÉRÉE COMME L'APPLICATION MODERNE DE CE QU'AFFIRMAIT M. LE JUGE FRANKFURTER IL Y A PLUSIEURS ANNÉES: (TRADUCTION NON OFFICIELLE) "L'HISTOIRE DE LA LIBERTÉ (AMÉRICAINNE) EST DANS UNE LARGE MESURE UNE HISTOIRE DE PROCÉDURE"¹⁶.

NOTES BIBLIOGRAPHIQUES

1. CE CHIFFRE EST TIRÉ DE: R. GRANT HAMMOND, "QUANTUM PHYSICS, ECONOMETRIC MODELS AND PROPERTY RIGHTS TO INFORMATION" (1981) 27 MCGILL L.J. 47 AT 48.
2. Y. MASUDA, THE INFORMATION SOCIETY AS POST-INDUSTRIAL SOCIETY (TOKYO: INSTITUTE FOR THE INFORMATION SOCIETY 1980) AT 114, 146.
3. H. BURKERT, "A FUNCTIONAL EXPLANATION OF DATA PROTECTION LAWS" (1982) COMPUTER L.J. 169.
4. S. BOK, SECRETS (NEW YORK: PANTHEON BOOKS, 1982), P. 19.
5. CANADA, MINISTÈRE DES COMMUNICATIONS ET MINISTÈRE DE LA JUSTICE, L'ORDINATEUR ET LA VIE PRIVÉE (OTTAWA: INFORMATION CANADA, 1971) P. 13-14.
6. ALAN F. WESTIN, PRIVACY AND FREEDOM (NEW YORK - ATHENUM PRESS, 1967) AT P. 7.
7. USCA S. 552 (B) (6).
8. EN VERTU DE L'ARTICLE 41 DE LA LOI AUSTRALIENNE SUR LA LIBERTÉ DE L'INFORMATION, SERAIENT EXEMPTS LES DOCUMENTS DONT LA DIVULGATION REPRÉSENTERAIT UNE DIVULGATION DÉRAISONNABLE DE RENSEIGNEMENTS PERSONNELS. CEPENDANT, LE PARAGRAPHE 41(2) PRÉCISE QUE CELA NE TOUCHE PAS LES DEMANDES SOUMISES PAR UNE PERSONNE EN VUE D'AVOIR ACCÈS AUX RENSEIGNEMENTS LA CONCERNANT. L'ARTICLE 45 CONSIDÈRE ÉGALEMENT COMME UNE EXCEPTION LA DIVULGATION D'UN RENSEIGNEMENT QUI CONSTITUERAIT UN ABUS DE CONFIANCE, CE QUI A ÉGALEMENT ÉTÉ INTERPRÉTÉ EN VUE DE PRÉSERVER LA VIE PRIVÉE. RÉCEMMENT, LA COMMISSION AUSTRALIENNE DE RÉFORME DU DROIT RECOMMANDAIT L'ADOPTION D'UNE LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS AFIN DE PRÉCISER LA PORTÉE DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET D'ÉTENDRE LE DROIT D'ACCÈS AU SECTEUR PRIVÉ, EN COMMENÇANT PAR LE TERRITOIRE DU COMMONWEALTH AUSTRALIEN.
9. ART. 19, LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS; ART. 13, LOI SUR L'ACCÈS À L'INFORMATION
10. S. BOK, OP. CIT., SUPRA NOTE 4, AT P. 13-14.
11. VOIR PARAG. 20(6), LOI SUR L'ACCÈS À L'INFORMATION.
12. LA PREMIÈRE AFFAIRE JUGÉE EN VERTU DE LA LOI SUR L'ACCÈS À L'INFORMATION SOULEVAIT JUSTEMENT CE GENRE DE QUESTION: MAISLIN INDUSTRIES LTD. V. MINISTRE DE L'INDUSTRIE ET DU COMMERCE ET AL (COUR FÉDÉRALE, DIVISION DE PREMIÈRE INSTANCE PER JEROME, A.C.J., LE 9 MAI 1984).

13. LE PARAGRAPHE 8(2) DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ÉNUMÈRE 13 GRANDES CATÉGORIES DANS LESQUELLES LA COMMUNICATION DES RENSEIGNEMENTS PERSONNELS À DES TIERCES PARTIES EST AUTORISÉE.
14. C. BAY - "COMMENT", IN J.D. MCCAMUS, FREEDOM OF INFORMATION : CANADIAN PROSPECTIVES (TORONTO: BUTTERWORTHS, 1981), P. 23
15. VOIR L'ÉTUDE PERTINENTE DANS: JOHN NAISBITT, MEGATRENDS (NEW YORK: WARNER BOOKS, 1984), P. 197.
16. MALINSKI V STATE OF NEW YORK (1945), 324, U.S. 401, 411, (FRANKFURTER, J.).

CP 1

E4

C62

INTERPROVINCIAL CONFERENCE ON PRIVACY:
INITIATIVES FOR 1984 (SYMPOSIUM)

Privacy Issue: The Property & Casualty Insurance Industry

James L. Kirschbaum
Chairman & C.E.O. of
Fireman's Fund Insurance Company of Canada and
Chairman of the
Automobile Committee of the Insurance Bureau of Canada



Toronto, Ontario
May 23-24, 1984

PRIVACY ISSUE: THE PROPERTY & CASUALTY INSURANCE INDUSTRY

PRESENTED WEDNESDAY, MAY 23, 1984 AT THE "CONFERENCE ON PRIVACY: INITIATIVES FOR 1984" SYMPOSIUM - SHERATON CENTRE, TORONTO, ONTARIO, BY JAMES L. KIRSCHBAUM, CHAIRMAN & C.E.O. OF FIREMAN'S FUND INSURANCE COMPANY OF CANADA AND CHAIRMAN OF THE AUTOMOBILE COMMITTEE OF THE INSURANCE BUREAU OF CANADA

Four years ago I arrived in Toronto. Believe it or not my wife's primary motivation in agreeing to the move was the fact I could use the transit system as an alternative to a busy freeway. So blissfully I headed for the subway station for my first day in the office. Since I had an empty briefcase I stopped and purchased a newspaper. Settling back to enjoy the leisure and the news, I was amused to read the headline "Insurance Companies Now Want to Know About Your Sex Life".

My amusement turned to shock when I discovered the insurance company was none other than my own, Fireman's Fund of Canada. The story was picked up all across North America and needless to say, the first day on the job turned out to be vastly different than originally planned. Actually, our program was a pretty good one -- psychological testing of impaired drivers. The self-administered tests were designed to separate the person who learned his lesson from the chronic drinking driver. Before the day was out I was in Frank Drea's office -- he was then the appropriate Minister.

Once we cleared the initial emotional issue with reporters, the only unanswered questions had to do with -- the use, the control and the safeguarding of the information gathered.

I was pleased to learn we had carefully considered the privacy issue. Our insureds completed the questionnaires and returned them direct to us in a specially addressed envelope. One person received them and opened and evaluated them one by one. The evaluation rating only was sent to the underwriter who never did see any of the information. All the responses and results were kept in a locked file to which no one else had access.

As part of my orientation and because of this experience I was pleased to learn the company had a very comprehensive written privacy code. This is gone over with all employees on hire and periodically thereafter. It has been reviewed from time to time for adequacy and application and so far has proven to be very effective.

It is a pleasure to be a participant in this conference and to have this opportunity to represent the Insurance Bureau of Canada. The latter is an organization consisting of 95 companies and company groups who write approximately 80% of all the Property & Casualty business in Canada.

In turning back the clock some ten or fifteen years ago, the whole subject of this conference was of major concern to many. At that time increased computer usage was coming in to vogue which triggered a rush to gather new and expanded data. Secondly, occurrences at the time,

coupled with events of the then recent past, were being interpreted as or associated with perceived improper gathering and use of information. For example, in many parts of the world there were lingering memories of World War II and the adverse impact information, whether right or wrong, could have on individuals or even entire nations. In the U.S., disclosures about FBI and CIA activities and the Watergate incident helped focus attention sharply on the whole subject.

Many very significant changes have occurred in the Property & Casualty Industry since 1970 as respects information. Contrary to initial concerns or even fears, the age of computerization has not led to problems and abuses. In fact, just the opposite has occurred.

With changed environmental factors, acceptance of different social and behavioural conducts and relationships, new underwriting concepts and techniques, the need to have so called private and personal information about insureds and/or applicants has changed dramatically. Twenty years ago, underwriters ordered and maintained reports on nearly all individual insureds. These were obtained through independent investigative firms who reported the information from file data and interviews of neighbours and business associates of the insured. Reports were generally fairly lengthy and often very subjective and new ones were periodically ordered with cumulative files maintained.

Presently such reports are very objective and consist largely of factors which are readily adaptable to computer application such as motor vehicle convictions. They are still ordered through independent investigative firms who now nearly always interview the insured or applicant directly and rarely will go to others. The reports are used primarily for confirmation or verification purposes and most companies order them on a fairly small percentage of their insureds.

In the Property & Casualty business, underwriters rarely obtain and use medical information. In those limited instances when they do, physician reports are requested directly through the insured. Most such requests involve automobile insureds and the reports are obtained to verify their current physical condition as it would pertain to their ability to safely operate a vehicle.

Both claim and underwriting files, whether electronic or hard copy, are treated on a very confidential need to know access basis. Further, the employment of such data has been cut back significantly hence the frequency of utilization of files has dropped dramatically. Accordingly, files are simply not out being reviewed and worked on to the extent they were in the past thus reducing potential unauthorized exposure.

In addition, the use of new sophisticated computer security systems, for the data stored electronically, ensures the availability on a "need to know" basis within a company.

Underwriting reports are still referred to as credit reports but it is a generic term only. The so called underwriting credit report usually doesn't provide indepth financial or credit information about a policyholder but rather deals only with information pertaining to the ownership and/or use of the vehicle and factors which reflects the driving experience and/or record of the insured.

With respect to claims, outside reports are ordered on a very small percentage of cases. When they are, they deal directly with some element of the adjustment process which requires outside review and/or verification. They could deal with specifics relative to an individuals financial position since that could have a direct bearing on the settlement process. Also, Claims Adjusters will on occassion order surveillance investigations. These are to determine or verify the degree to which somebody might be disabled or the extent of injury or damage.

A very decided change has taken place relative to the gathering and sharing of medical information as respects claims. The Industry practice is to obtain and/or share only with the written consent of the insured or third party. Frequently this information is done on a physician to physician basis. Such information and results are treated on a particularly confidential basis with only very limited access. Adjusters today will confirm existence of an injury, for example, but will not share medical information with others unless authorized to do so in writing by the injured party.

There are some misconceptions about the amount of information Insurance companies have on people and the degree to which that is shared. There simply aren't any large information data bases in existence either overall or within specific companies. Most companies still do not have very sophisticated linkage of data internally and literally nothing in the way of linkage exists on a multi-company basis. About the only information shared, and this is on a very informal and limited basis, is specific experience information or claims history. The Industry does share premium and claims information for overall statistical purposes but this is not by individual insured. Also, where evidence points to potential fraud or other potential criminal activity a company may provide information to an Industry sponsored crime bureau. Such cases are fortunately very limited. This organization is staffed with professionals who work very closely with law enforcement agencies.

Some people are under the impression Insurance companies sell lists of customers to others. We certainly do not and to date I have been unable to come up with a single other company which employs that practice. Also, some people have expressed concerns about what they perceive is the improper use of telephone soliciting. Some agents and brokers do use the telephone extensively for solicitations. The practice however is fairly limited and has been going on for decades.

With respect to personnel files, I again found significant change especially with regard to what information was collected and how such information was maintained. Because of the dramatic changes in this regard, personnel files today are much slimmer than they were previously. Again, very tight security is maintained.

Quite frequently people will call requesting information about our people. We have a very formal and rigid policy about this and simply do not respond unless authorized by the employee involved to do so.

Since we operate basically in a "white collar" environment, our Workers' Compensation exposures are minimal and we simply don't have medical files on our employees.

Companies now make provision throughout for easy correction to any misinformation which may be developed. With a voluntary access program to one's personnel file, we have experienced minimal numbers of requests from people to examine our files on them. My people feel this is in part due to the fact that some don't understand their priviledges while most aren't interested.

SUMMARY AND CONCLUSION:

As I stated earlier, the means to share massive amounts of personal information simply does not exist in our Industry. More importantly, we and our fellow Insurers collect far less information today than we did a few years ago, gather it in an improved manner and have formulated policies to safeguard what we do collect.

Insurance companies have operated for centuries in a fiduciary capacity. While concern for the privacy of individuals is a comparatively recent phenomenon, it has been handled by the general insurance companies as

another of the many areas in which they must protect the interests of their customers, and their employees.

It is our belief the industry is thoroughly aware of the issue of privacy and has responded very aggressively and positively. Even in situations where alleged deficiencies or abuses existed and these were very minimal, the Industry responded quickly and positively to remove any such real or alleged shortcomings. Symposiums of this nature are helpful since they serve as reminders and also may surface areas which could benefit from additional attention, however we do not believe any additional regulations or legislation are necessary.

It has been a pleasure being part of this conference. Thank you for inviting me.

CAI
74
-C52

DOCUMENT: 870-123/012

CONFÉRENCE INTERPROVINCIALE SUR LA PROTECTION DES
RENSEIGNEMENTS PERSONNELS: MESURES POUR 1984 (COLLOQUE)

La protection des renseignements personnels:
l'industrie de l'assurance risques divers

James L. Kirschbaum

Président et administrateur en chef de la compagnie d'assurance
Fireman's Fund du Canada et président du Comité sur l'automobile
du Bureau d'assurance du Canada

Toronto (Ontario)

Les 23 et 24 mai 1984



LA PROTECTION DES RENSEIGNEMENTS PERSONNELS: L'INDUSTRIE DE
L'ASSURANCE RISQUES DIVERS

PRÉSENTATION LE MERCREDI 23 MAI 1984 À L'ATELIER DE LA "CONFÉ-
RENCE SUR LA VIE PRIVÉE: PROJETS POUR 1984" TENU AU CENTRE
SHERATON, À TORONTO (ONTARIO), PAR JAMES L. KIRSCHBAUM, PRÉSIDENT
ET ADMINISTRATEUR EN CHEF DE LA COMPAGNIE D'ASSURANCE FIREMAN'S
FUND DU CANADA ET PRÉSIDENT DU COMITÉ SUR L'AUTOMOBILE DU BUREAU
D'ASSURANCE DU CANADA

Il y a de cela quatre ans j'arrivais à Toronto. Croyez-le ou non, la principale raison pour laquelle ma femme a accepté de déménager était le fait que je pourrais utiliser le transport en commun au lieu de ma voiture. C'est donc en toute quiétude que je me suis dirigé vers une station de métro pour mon premier jour de travail. Étant donné que ma serviette était encore vide, je suis arrêté à un kiosque pour y acheter le journal. Tout heureux d'avoir le temps de lire les nouvelles, c'est avec amusement que j'ai remarqué le titre "Insurance Companies Now Want to Know About Your Sex Life" (Voilà que les compagnies d'assurance veulent en savoir plus long sur votre vie sexuelle).

Mon amusement s'est vite transformé en stupéfaction lorsque j'ai découvert que la société d'assurance dont il était question

n'était nulle autre que la mienne, la Fireman's Fund du Canada. L'histoire a fait le tour de l'Amérique du Nord et il va sans dire que ma première journée de travail ne s'est pas du tout déroulée comme je l'avais prévu. En fait, notre programme n'était pas mal du tout, il s'agissait d'une mise à l'épreuve psychologique des personnes ayant conduit avec des facultés affaiblies. Les tests, administrés par la personne elle-même, visaient à distinguer chez les conducteurs visés les personnes qui avaient appris leur leçon des buveurs invétérés. Avant la fin de la journée, j'étais dans le bureau de Frank Drea, qui était le ministre responsable à l'époque.

Une fois que nous avons réussi à expliquer toute cette délicate question aux journalistes, les seules questions restées sans réponse concernaient l'utilisation, le contrôle et la protection des renseignements recueillis.

J'ai pu avec plaisir constater que nous avons soigneusement étudié la question de la protection des renseignements personnels. Nos assurés remplissaient leurs questionnaires et nous les renvoyaient directement dans des enveloppes spécialement adressées qu'une personne recevait, ouvrait et évaluait une par une. Seul le pointage qui résultait de l'évaluation était envoyé

au tarificateur qui ne voyait aucun des renseignements. Tous les résultats et réponses étaient gardés dans un classeur verrouillé auquel personne d'autre n'avait accès.

En raison de ma formation et aussi à cause de cette expérience, j'ai été heureux d'apprendre que la société disposait d'un code écrit exhaustif sur la protection des renseignements personnels. Ce code est passé en revue avec tous les employés au moment de leur embauche et périodiquement par la suite. Il a été révisé de temps à autre pour des questions de mise à jour et d'application et il s'est révélé jusqu'ici très efficace.

Je suis vraiment heureux de participer à cette conférence et d'avoir l'occasion d'y représenter le Bureau d'assurance du Canada. Cette organisation comporte 95 sociétés et groupes sociétaires qui représentent approximativement 80 p. 100 des groupes d'assurance risques divers au Canada.

Si nous retournons de dix à quinze ans en arrière, nous pouvons constater que ce qui fait l'objet de la présente conférence constituait alors pour beaucoup une importante source de préoccupation. À cette époque, l'usage accru des ordinateurs prenait de l'ampleur, ce qui provoquait une véritable ruée vers la collecte de données nouvelles et plus détaillées. En second lieu, certains faits de l'époque, associés à des événements récents à

ce moment-là étaient interprétés ou perçus comme des activités indues de collecte et d'utilisation d'information. Par exemple, dans plusieurs parties du monde subsistait le souvenir de la Seconde Guerre mondiale et des effets néfastes qu'une information bonne ou mauvaise pouvait avoir sur des particuliers, voire sur des nations entières. Aux États-Unis, les divulgations relatives aux activités du FBI et de la CIA ainsi que l'incident du Watergate ont contribué à attirer fortement l'attention sur toute la question.

Bon nombre de changements significatifs sont survenus dans l'industrie de l'assurance risques divers depuis 1970 en ce qui a trait à l'information. Contrairement aux craintes voire aux peurs initiales, l'ère de l'informatisation n'a provoqué ni problèmes ni abus. En fait, c'est justement le contraire qui s'est produit.

En raison de la transformation du milieu, de l'acceptation de conduites et de relations différentes en matière de société et de comportement, et de nouveaux concepts et techniques de tarification, la nécessité d'obtenir des renseignements dits privés et personnels au sujet des assurés ou de ceux qui faisaient une demande d'assurance s'est radicalement transformée. Il y a vingt ans, les assureurs commandaient et conservaient des rapports sur presque toutes les personnes assurées. Ceux-ci étaient obtenus

par l'intermédiaire d'enquêteurs indépendants qui fondaient leur rapport sur des données en dossier et sur des entrevues réalisées auprès de voisins ou d'associés de l'assuré. Les rapports étaient généralement fort longs et souvent très subjectifs et de nouveaux comptes rendus étaient périodiquement commandés, ce qui supposait le maintien de dossiers cumulatifs.

À l'heure actuelle, les rapports de ce genre sont très objectifs et consistent essentiellement en facteurs qui sont facilement adaptables à un usage informatisé, par exemple les condamnations relatives à des infractions au code de la route. Ces rapports sont encore demandés à des entreprises privées d'investigation qui, de nos jours, interrogent presque toujours directement l'assuré ou la personne qui fait une demande d'assurance, et s'adressent rarement à d'autres personnes. Les rapports sont principalement utilisés à des fins de confirmation ou de vérification et la plupart des compagnies n'en font dresser que pour un très faible pourcentage de leurs assurés.

Dans le secteur de l'assurance risques divers, les assureurs obtiennent et utilisent rarement des renseignements d'ordre médical. Dans les rares cas où cela se produit, les rapports du médecin sont demandés directement par l'intermédiaire de l'assuré. La plupart de ces demandes touchent des automobilistes

et les rapports servent à vérifier leur état de santé actuel dans la mesure où il touche leur aptitude à conduire un véhicule en toute sécurité.

Les dossiers de réclamation et de tarification, qu'ils soient électroniques ou manuels, sont traités d'une façon très confidentielle en fonction de ce que les intéressés ont vraiment besoin de savoir. De plus, l'emploi de ces données a été considérablement réduit, ce qui a radicalement diminué la fréquence d'utilisation des dossiers. Par conséquent, on révise ou utilise les dossiers beaucoup moins fréquemment que par le passé, ce qui réduit les perspectives de divulgation non autorisée.

En outre, l'utilisation de nouveaux systèmes perfectionnés de sécurité pour les ordinateurs, dans le cas des données entreposées électroniquement, limite la divulgation des données aux personnes qui en ont vraiment besoin au sein de la compagnie.

Les rapports d'assurance sont souvent encore appelés des rapports de crédit, mais il ne s'agit là que d'un terme générique. Ce qu'on désigne sous le nom de rapport de crédit ne fournit en général pas de renseignements détaillés au sujet de la situation financière ou du crédit d'un détenteur de police mais traite

plutôt de renseignements relatifs à la propriété ou à l'utilisation d'un véhicule et de facteurs qui traduisent l'expérience ou le dossier de l'assuré dans le domaine de la conduite automobile.

En ce qui a trait aux réclamations, des rapports ne sont commandés à l'extérieur que pour un très faible pourcentage de cas. Ils traitent alors directement d'un élément précis du processus d'ajustement qui nécessite une revue ou une vérification externe. Ils peuvent porter sur des détails relatifs à la situation financière d'une personne puisque cela peut avoir un lien direct avec le processus de règlement. De plus, les ajusteurs d'assurance commandent à l'occasion des enquêtes de surveillance. Celles-ci ont pour but de déterminer ou de vérifier dans quelle mesure quelqu'un peut être handicapé ou encore l'étendue de la blessure ou du tort subi.

Un changement déterminant est survenu en matière de collecte et de partage de données médicales touchant des réclamations. L'industrie a comme règle de n'obtenir ou de ne partager ces renseignements qu'avec le consentement écrit de l'assuré ou de la tierce partie. Fréquemment, ce type de renseignement est transmis de médecin à médecin. Ce genre d'information et les conclusions qu'elle entraîne sont traitées de façon particulièrement confidentielle en fonction d'un accès très limité. Ainsi, les ajusteurs actuels peuvent confirmer l'existence d'une blessure

mais ne donneront aucun renseignement d'ordre médical à d'autres personnes à moins d'y être autorisés par écrit par la partie lésée.

Il existe certaines idées fausses quant au volume et au partage de l'information que les sociétés d'assurance détiennent au sujet des gens. En réalité, il n'existe aucune base de données importante, que ce soit dans l'ensemble ou au sein de sociétés précises. La plupart des sociétés ne disposent pas encore d'un système très perfectionné de recoupage des données dans leurs services internes et il n'existe rien de comparable à une interconnexion entre plusieurs sociétés. Les seuls renseignements qui sont partagés et ce, d'une façon très limitée et pas du tout officielle, consistent en des renseignements précis sur certaines expériences ou des dossiers touchant les réclamations. Certes, l'industrie partage des renseignements sur les primes et les réclamations à des fins statistiques générales mais ce calcul ne s'effectue pas par individu assuré. De plus, lorsque tout porte à croire à une fraude éventuelle ou à d'autres activités criminelles, une société peut fournir des renseignements à un bureau d'investigation parrainé par l'industrie. Heureusement, ces cas sont très rares. Cette organisation est dotée d'un personnel professionnel qui travaille en étroite collaboration avec les organismes chargés de l'application de la loi.

Certaines personnes ont l'impression que les sociétés d'assurance vendent des listes de clients à d'autres organismes. Cela est tout à fait faux dans notre cas et jusqu'ici je ne connais pas encore une seule autre société qui ait recours à cette pratique. Par ailleurs, certains ont exprimé leurs préoccupations face à ce qu'ils perçoivent comme une utilisation induite des requêtes par téléphone. Certains agents et courtiers se servent énormément du téléphone pour pressentir des gens. Cette pratique est cependant relativement limitée et a cours depuis des décennies.

En ce qui a trait aux dossiers personnels, j'ai également constaté des changements importants, en particulier par rapport aux types de renseignements recueillis et au mode de conservation des données. En raison de l'évolution radicale qui est survenue à cet égard, les dossiers personnels sont aujourd'hui beaucoup moins volumineux qu'auparavant. Là encore, une sécurité très forte est assurée.

Il arrive souvent que des gens nous appellent pour nous demander des renseignements au sujet de notre personnel. Notre politique à cet égard est très officielle et stricte au point que nous ne donnons pas suite à ces requêtes sauf si l'employé concerné nous l'y autorise.

Étant donné que nos employés sont essentiellement du personnel de bureau, les cas relatifs à l'indemnisation des travailleurs sont infimes et nous ne tenons simplement pas de dossiers médicaux au sujet de nos employés.

De nos jours, les sociétés prévoient une correction facile de tout mauvais renseignement. En dépit d'un programme volontaire d'accès aux dossiers individuels, nous avons reçu très peu de demandes de personnes désireuses d'étudier les dossiers les concernant. Mon personnel estime que cela est attribuable en partie au fait que certains ne comprennent pas leurs privilèges tandis que la plupart ne sont pas intéressés.

RÉSUMÉ ET CONCLUSION

Comme je l'ai déjà mentionné, notre industrie ne dispose tout simplement pas des moyens de partager des quantités massives de renseignements personnels. Fait plus important encore, notre société et nos collègues des autres compagnies d'assurance recueillons bien moins d'information aujourd'hui que cela n'était le cas il y a quelques années à peine, nous les recueillons d'une façon améliorée et nous avons formulé des politiques pour protéger les renseignements que nous recueillons.

Les compagnies d'assurance exercent depuis des siècles la fonction de fiduciaire. Même si le souci de la protection de la vie privée des personnes constitue un phénomène relativement récent, il n'en a pas moins été traité par les sociétés d'assurance générale comme l'un des nombreux domaines dans lesquels elles doivent protéger les intérêts de leurs clients ainsi que leurs employés.

Nous croyons que notre industrie est parfaitement consciente du problème de la protection des renseignements personnels et qu'elle y a fait face de façon très dynamique et positive. Même dans les situations dans lesquelles des lacunes ou des abus présumés se sont concrétisés, et ces cas ont été très rares, l'industrie a réagi promptement et catégoriquement afin de corriger ces lacunes réelles ou présumées. Les colloques comme celui-ci sont utiles car ils servent un peu d'aide-mémoire et peuvent également permettre de déceler des secteurs qui demandent plus d'attention, mais nous ne croyons cependant pas à la nécessité de règlements ou de lois supplémentaires.

Je suis très heureux de participer à cette conférence. Merci de m'avoir invité.

DOCUMENT: 870-123/013

CA1
E4
-C52

INTERPROVINCIAL CONFERENCE ON PRIVACY:
INITIATIVES FOR 1984 (SYMPOSIUM)

Privacy: The Problems Defined

Ross W. McFarlane, Q.C.



Toronto, Ontario
May 23-24, 1984

"CONFERENCE ON PRIVACY: INITIATIVES FOR 1984"

PRIVACY: THE PROBLEMS DEFINED

Introduction

Hugh Rowan pointed out in his paper "Privacy and the Law",¹ that one of the difficulties besetting any discussion of privacy is the meaning or definition of the word "privacy" itself. Privacy is an intensely personal or subjective value - what one person would regard as intolerable, another would dismiss as a minor irritant.

A 1979 Harris poll conducted in the U.S. revealed the following major findings, concerning employee privacy issues:

Twenty-five percent of the public believed employers asked for too much personal information;

Almost a third of the public believed business did not do enough to keep employee information confidential;

Seventy percent of employees believed laws should be passed giving employees a right of access to their personnel files;

Ninety-three percent of employees believed employers should adopt specific policies to safeguard the information in employee personnel and medical files;

Ninety-one percent of employees believed employers should be required to inform employees of any information indicating that the health of employees is being affected by conditions at work.

Several Canadian provinces have enacted legislation protecting individual privacy and creating a tort of invasion of privacy - without proof of actual damage. Initially hailed as a significant legal development, the passage of these privacy acts has really been a non-development according to Professor Peter Burns of the U.B.C. Law School in his article entitled the "Law and Privacy: the Canadian Experience".²

The high cost of litigation and the embarrassment of having the invasion made public has deterred individuals from using the legislation. Therefore the Acts have not provided real protection to privacy interests.

R. Dale Gibson, Professor of Law at the University of Manitoba in his article "Legal Protections of Privacy" suggests that "the main explanation for the limited impact of privacy statutes is probably that there are not many forms of privacy invasion which are not already well protected by existing legal or social sanctions."³

I've mentioned some of the privacy concerns of employees what are some of the privacy problems of business?

1. Access to Employee Medical Records

Surprisingly, a concern for corporations is the inability of management to get access to employee medical records held by its own company physicians. Companies, through their medical departments, acquire a great deal of medical information about an employee during the course of his or her employment.

It is common for employees to put forward their medical condition as an important factor in disputes with their employer. Normally in a civil action, the opposite party can obtain copies of relevant hospital and medical records pursuant to the rules of practice of the court. This is done to avoid

surprises at trial and minimize wasting the court's time. Ontario courts have gone as far as to say that non-disclosure of relevant medical records to the opposite party would be scandalous.⁴

Similarly, in employee-employer disputes, management would like to receive relevant medical information that has been obtained by the company's physicians, in order to determine whether the employee's claim is legitimate. The current medical-legal climate, however, seems to promote non-disclosure. The result can be trial by ambush for corporations.

How does this happen? Lets assume an employee-employer dispute occurs in a corporation. It can happen in a variety of ways, for example:

1. An employee is fired for refusing to perform his employment duties. The employee says he is sick or injured and can't carry out the work; or
2. An employee claims that he is eligible for certain disability benefits which are dependent on his medical record; or

3. An employee applies for a transfer to a different job in the company which is refused because the company doctor says the employee is unable to do the the work.

So the employer approaches its company physician requesting access to the employee's medical files. Surprisingly, the company physician bluntly refuses to disclose the information.

The Physician's refusal is based upon the Ontario Health Disciplines Act; which defines "Professional misconduct" to mean:

"giving information concerning a patient's condition or any professional services performed for a patient to any person other than the patient without the consent of the patient, unless required to do so by law."⁵

Obviously, the employer is placed at a serious disadvantage in resolving this type of conflict, if the employee refuses to permit the doctor to disclose the medical information. Further, if proceedings result, the employer will not see the medical records until the day of the hearing.

The employee's representatives have all of the necessary medical information relating to the employee's claim including reports, and records prepared by the company's doctors. This is manifestly unfair to the employer, who is compelled to wait until the day of the hearing and is therefore unable to adequately prepare its case.

On the other hand, if the employer had been shown the medical information when the complaint first arose, the employer aware of the specific evidence of an employee's serious medical condition would presumably resolve the dispute quickly, sparing both parties the time and expense of a needless hearing.

There is obviously an area of conflict between the duty which a company physician owes to his employer and his statutory duty to persons consulting him in a professional capacity.

The Krever Commission Report into the Confidentiality of Health Information focused on this problem.

It recommended that legislation be enacted "to make it clear that a professional employee's duty of confidentiality

transcends his or her duty to obey an employer's instructions, where those instructions require the employee to reveal information held in confidence."⁶

The 1980 Ontario Court decision involving Dr. Morton Shulman reinforces the point that it is a physician's duty not to disclose patient information even if such disclosure would serve a high social purpose .⁷

We can all foresee situations where the need for privacy should yield to a public interest need for disclosure. One such situation arises where the company physician is of the opinion that an employee would jeopardize his own health or safety, or that of his co-workers, if he continued to perform his assigned tasks.

An example is an employee engaged in the assembly of automobiles, who is subject to dizzy spells. Section 15 of the Ontario Occupational Health and Safety Act places a statutory duty on employers to "take every precaution reasonable in the circumstances for the protection of a worker".

Another example arises where a company doctor becomes aware that the blood lead levels of certain employees exceed permissible

levels, suggesting that these employees may be exposed to high concentrations of lead. The doctor is entitled to indicate to plant management that there are excessive lead levels in the plant, but is precluded from disclosing which particular employees are affected. Management is therefore unable to take effective action to remedy a potential hazardous situation in the plant.

If employers are to properly discharge their obligations under the Occupational Health & Safety Act to protect workers in the workplace, they must have specific information concerning health or safety risks, including the medical information about the employee's involved.

It is clear that amending the Health Disciplines Act to permit some disclosure of medical information is necessary and desirable in these cases.

2. Surveillance

Should companies faced with the inability to obtain medical evidence prior to a hearing, engage in employee surveillance to produce the necessary information? This is particularly so in

workmen's compensation cases where the employer knows, or strongly suspects, the employee is a malingerer but cannot otherwise produce the evidence.

The introduction of photographs or video tapes of the employee's activities into evidence may prevent an unqualified claimant from receiving benefits. The admissibility of such evidence is a matter for the presiding judge or tribunal.

Covert surveillance activities obviously impacts upon an employee's privacy. However provided there is no trespass or intimidation involved, such activities do not appear to be prohibited by the criminal law.

As mentioned, several Canadian Provinces have passed privacy legislation creating a tort for the unreasonable violation of a person's privacy. The Saskatchewan and Newfoundland Acts specifically state that auditory or visual surveillance of a person by any means whether or not accompanied by trespass, is prima facie a violation of privacy.

While no one would disagree with the intent of this legislation to protect people from unreasonable violations of their privacy, it can tie the hands of a company who has an employee who is abusing the system and unfairly collecting workmen's compensation benefits.

3. Personnel Files - Collection, Storage and Distribution of Employee Information

Employers collect personally identifiable employee information for a variety of business reasons, such as the proper administration of labour agreements, benefit programs and other business functions or to comply with various federal and provincial laws and regulations. Personally identifiable information includes any information about an employee that can be isolated, such as a name, employee serial number or social insurance number.

There is no question that there has been increased emphasis within corporations on the fair treatment of employee's records, their confidentiality, accuracy and relevance.

We have found fair information practices and concern for protecting personal employee information to be consistent with good business practices.

In my experience major corporations have procedures, or "Codes of Conduct" which would include most of the following guidelines, for the protection of employees information:

1. Collection and Use of Data

Only such information as is relevant and necessary to the employment relationship should be collected. No records should be gathered or maintained concerning an employee's political activities, memberships, publications or communications of non-employment activities without the written authorization of the employee.

Access to personal employee information should be limited to those persons in the company having a legitimate need for such information in the performance of their job responsibilities. Employees using such information should be instructed as to the importance of maintaining the confidentiality of personal employee information.

All notes, memoranda and letters generated by management and contained in personnel files should be written in a straight forward, objective manner.

2. Disclosure of Information Outside the Company

Personal employee information should not be disclosed outside the company without the employee's written consent, unless required to be disclosed by law or by court order.

The need to regulate disclosure to third parties is becoming more apparent as corporations are increasingly seen to be information sources for parties engaged in, or contemplating litigation. Inquiries include the following:

- (a) summary of an employee's work record;
- (b) previous periods of absence;
- (c) availability of overtime hours;
- (d) physical requirements for a specified job;
- (e) location of an individual;
- (f) personal medical information;
- (g) rates of pay and expected increases in pay.

This information should not be disclosed without the consent of the employee concerned.

In a typical situation, information concerning an employee's income is requested by his or her spouse in family court support proceedings. Following company policy, the request is denied and the spouse then proceeds to subpoena the records. The result can be that companies may find their personnel administrators spending almost as much time in court as at the office. Where medical information is requested, the personnel administrator will not have the medical record, with the result that a company can end up with two employees in court, the personnel administrator and the company doctor.

Legislation allowing employers reasonable compensation for their time and expense associated with these information requests would reduce these costs and help eliminate unnecessary requests.

(3) Employee Access to Personnel Files

There is increasing pressure on companies to give employees access to their personnel files. This is seen to be a corollary

right to the right of privacy in the files. The federal Privacy Act includes provisions for access to personal information held by a federal government institution about individuals. Recently, a Private Members Bill was introduced in the Ontario legislature amending the Employment Standards Act to give employees in Ontario the right of access to employer's personnel records relating to the employee.⁸

I believe, most businessmen support the principle that employees should have access to their personnel records. It is my experience that employees rarely exercise this right, since most companies now disclose to their employees the employee's performance evaluation rating, during the appraisal process.

4. Privacy of Confidential Technical Information of Suppliers

The transfer of technical information between an owner and a user of the information is common in the high-tech, specialized business environment of the 1980's. Large, diversified multi-national corporations rely on technology developed by outside firms specializing in intellectual property. This property may take the form of computer software, blue prints and drawings, video tapes, audio cassettes, and so on. A privacy

concern arises out of the supplier's desire to protect from public disclosure what may be his only major asset - the technical information.

In order to protect its interests in the property, the supplier of the information looks to patent, trade mark, copyright and industrial design laws. Most view such laws ineffective or inadequate in protecting its valuable information.

Accordingly, suppliers are increasingly seeking to obtain contractual protection for their confidential information through non-disclosure agreements. These agreements permit the supplier to impose upon the recipient far reaching obligations. Recipient companies should be cautious when signing non-disclosure agreements.

The agreements should be for a limited period of time, should only cover written communications and should define the standard of care to be provided by the recipient company. For example the recipient company could agree to give the information the same protection as it does to its own confidential information.

A new twist to the protection of supplier trade secrets and confidential information involves the developing Canadian Workplace Hazardous Materials Information System. Industry, labour and government have worked to develop a system which would permit suppliers of hazardous materials to disclose information about these products to the users, while still protecting the supplier's trade secrets in this information. The information is required by the users to educate their employees on the safe use of hazardous materials in the workplace.

Implementation of this system will balance the conflicting needs of providing the information so that the user can educate his employees, against the supplier's vital interest in protecting its trade secrets.

5. Confidentiality of Business Information

Just as individuals are concerned about the confidentiality of their personal records, companies take great care to protect their confidential business information from disclosure to their competitors and to the public.

As many of you are aware, on July 1, 1983 the Federal Access to Information Act came into force. The laudable objectives of promoting open and accountable government have come under close scrutiny by the private sector whose confidential records, in the hands of government agencies, become subject to public disclosure.

Several provincial governments have passed, or like Ontario are considering the passage of similar legislation governing public access to provincial government records.

The past ten months' experience under the AIA indicates that companies have or should become more cautious in their dealings with the federal government out of fear that confidential information will be subject to public disclosure. Relations with government which were once less formal have become formalized; both parties require information requests be put in writing; replies are scrutinized and documents painstakingly stamped "confidential". The exchange of information between business and government now follows rigid guidelines.

The recent Federal Court of Canada Maislin Transport decision suggests that the private sector's concerns are not

ill-founded. It is difficult to fully appreciate the significance of this case, because we don't know what the specific financial information Maislin argued was confidential and therefore should not be disclosed.

However it is clear from the decision that "it is not enough for Maislin to treat the information confidentially, but it must in fact be confidential by some objective standard."

The objective standard the court appears to be applying is the U.S. National Parks vs Morten test which held that in order for the information not be disclosed it must "cause substantial harm to the competitive position of the person from whom the information was obtained."

A U.S. critic stated that the substantial competitive injury test places an almost impossible burden of proof on the submitter. Also gathering the evidence required to keep documents from exposure is so costly only the largest corporations make the effort.⁹ *place in the*

It is hoped that if Ontario introduces freedom of information legislation that it does not impose standards of disclosure that are so onerous as to dissuade companies from freely communicating with their government, out of fear of disclosure of their sensitive information.

Conclusion

The presence of sophisticated electronic equipment used in business today permits information to be collected, collated and distributed quickly and to various recipients. Such capabilities are required to be competitive in today's global economy. What is needed is a balancing of the interests of all parties involved - a delicate balance which will protect the rights of all parties, yet permit the use of society's most valuable resource - information. That is the challenge for government and business today.

R. W. McFarlane, Q.C.

May 23, 1984

FOOTNOTES

1. Hugh Rowan, Q.C., "Privacy and the Law", Law Society of Upper Canada Special Lectures, 1973, pp. 259-307.
2. Peter Burns, "The Law and Privacy: The Canadian Experience", (1976), 54 Canadian Bar Review 1.
3. R. Dale Gibson, "Legal Protections of Privacy", The Practice of Freedom, Canadian Essays on Human Rights and Fundamental Freedoms, 1979.
4. Coderque v Mutual of Omaha Insurance Co., [1970] 1 O.R. 473 (Ontario Supreme Court).
5. Health Disciplines Regulations, R.R.O. 1980, Reg. 448, section 27(22).
6. Report of the Commission of Inquiry into the Confidentiality of Health Information, Volume III, pp. 167-168.
7. Re Shulman and College of Physicians & Surgeons of Ontario (1980), 29 OR (2d) 40 (Ontario Division Court).
8. Bill 20 - An Act to amend the Employment Standards Act (Reid, Rainy River).
9. Jack I. Pulley, Senior Environment Attorney Dow Corning Corporation, "The Freedom of Information Act - A Government Subsidy for Industrial Espionage." p.11

CA1

Z2

- C52

DOCUMENT: 870-123/013

CONFÉRENCE INTERPROVINCIALE SUR LA PROTECTION DES RENSEIGNEMENTS

PERSONNELS: MESURES POUR 1984 (COLLOQUE)

La protection des renseignements personnels:

Définition des problèmes

Ross W. McFarlane, c.r.



Toronto, Ontario

23-24 mai 1984

CONFÉRENCE SUR LA PROTECTION DES RENSEIGNEMENTS

PERSONNELS: MESURES POUR 1984

LA PROTECTION DES RENSEIGNEMENTS PERSONNELS:

DÉFINITION DES PROBLÈMES

Introduction

Dans son article intitulé "Privacy and the Law",¹ Hugh Rowan a souligné que l'une des difficultés qui complique tout débat sur la protection des renseignements personnels est la signification ou la définition de l'expression "protection des renseignements personnels" elle-même. La protection des renseignements personnels constitue une valeur extrêmement personnelle ou subjective: une personne considérerait intolérable ce qu'une autre jugerait simplement agaçant.

Un sondage Harris mené en 1979 aux États-Unis a révélé les principales conclusions suivantes sur la protection des renseignements personnels au sujet des employés:

Vingt-cinq pour cent des personnes interrogées pensaient que les employeurs demandaient trop de renseignements personnels;

Presque un tiers des personnes interrogées estimaient que les entreprises ne prenaient pas suffisamment de mesures pour assurer la confidentialité des renseignements détenus au sujet des employés;

Soixante-dix pour cent des employés pensaient qu'on devrait adopter des lois donnant aux employés le droit de consulter leur dossier personnel;

Quatre-vingt-treize pour cent des employés pensaient que les employeurs devraient adopter des lignes directrices spécifiques afin de protéger les renseignements contenus dans les dossiers personnels et médicaux des employés;

Quatre-vingt-onze pour cent des employés pensaient que les employeurs devraient être tenus d'informer les employés de tout renseignement indiquant que la santé des employés est menacée par ses conditions de travail.

Plusieurs provinces canadiennes ont adopté une législation assurant la protection des renseignements personnels et créant le délit d'atteinte à la vie privée, sans qu'il soit nécessaire d'établir l'existence d'un dommage. Initialement saluée comme une initiative juridique importante, l'adoption de ces lois sur la protection des renseignements personnels n'a pas eu en fait les résultats escomptés, selon l'avis exprimé par le professeur Peter Burns de la Faculté de droit de l'Université de Colombie-Britannique dans son article intitulé "Law and Privacy: the Canadian Experience".²

Le coût élevé des procédures judiciaires et l'embarras éprouvé en raison de la publicisation de l'atteinte en question dissuade les individus de se prévaloir de la législation. Par conséquent, ces lois n'assurent pas une réelle protection des renseignements personnels.

Dans son article intitulé "Legal Protections of Privacy", R. Dale Gibson, professeur de droit à l'Université du Manitoba avance que la principale explication à l'impact limité des lois sur la protection des renseignements personnels tient probablement au fait qu'il existe peu de formes d'atteinte à la vie privée qui ne soient déjà bien protégées par les sanctions légales ou sociales existantes."³

J'ai mentionné certaines préoccupations des employés en ce qui a trait à la protection des renseignements personnels; quels sont maintenant les problèmes du monde des affaires à cet égard?

1. Accès aux dossiers médicaux des employés

Il est surprenant de constater que les sociétés se plaignent du fait que leurs gestionnaires ne peuvent avoir accès aux dossiers médicaux des employés, détenus par les propres médecins des sociétés. Celles-ci, par le biais de leurs services médicaux, obtiennent une somme importante de renseignements médicaux sur les employés pendant qu'ils sont à leur service.

Les employés invoquent fréquemment leur état de santé comme un facteur important dans les litiges avec leur employeur. Normalement, dans une poursuite civile, la partie opposée peut obtenir copie des dossiers pertinents de l'hôpital et du médecin, conformément aux règles de pratique de la cour. On procède ainsi afin d'éviter les surprises lors du procès et de minimiser les pertes de temps devant le tribunal. Les tribunaux

ontariens sont même allés jusqu'à affirmer qu'il serait scandaleux de ne pas divulguer les dossiers médicaux pertinents à la partie opposée.⁴

Dans les litiges entre employeur et employés, la direction aimerait pareillement obtenir les renseignements médicaux pertinents recueillis par les médecins de la compagnie, afin de déterminer si la demande de l'employé est bien fondée. Toutefois, le climat actuel dans le domaine médico-légal ne semble pas s'y prêter. Il pourrait en résulter des procès-surprises pour les sociétés.

Comment cela peut-il se produire? Prenons l'hypothèse d'un litige entre employeur et employé dans une société. Celui-ci peut surgir de diverses façons; par exemple:

1. Un employé est congédié pour avoir refusé d'exécuter ses fonctions. L'employé déclare qu'il est malade ou blessé, et qu'il ne peut faire le travail; ou
2. Un employé soutient être admissible à certaines prestations d'incapacité, qui sont fonction de son dossier médical; ou
3. Un employé demande à être muté à un autre poste dans la compagnie, ce qui lui est refusé parce que le médecin de la compagnie déclare qu'il est incapable d'accomplir le travail.

L'employeur s'adresse donc à son propre médecin, demandant à consulter le dossier médical de l'employé, et constate avec surprise que le médecin refuse tout simplement de lui donner les renseignements.

Le refus du médecin est fondé sur la Loi sur les professions médicales et paramédicales de l'Ontario, qui définit ainsi l'expression "faute professionnelle"

"Le fait de donner des renseignements au sujet de l'état d'un patient, ou au sujet de tout service professionnel dispensé à un patient, à toute autre personne que le patient, sans le consentement de ce dernier, à moins d'y être obligé par la loi."⁵

De toute évidence, l'employeur se trouve en position d'infériorité pour résoudre ce genre de conflit, si l'employé refuse au médecin le droit de divulguer les renseignements médicaux. En outre, si des procédures judiciaires sont intentées, l'employeur ne pourra consulter le dossier médical avant le jour de l'audience.

Les représentants de l'employé ont tous les renseignements médicaux nécessaires au sujet de la demande de l'employé, y compris les rapports et les registres préparés par les médecins de la compagnie. Cette situation est manifestement injuste pour l'employeur, qui doit attendre jusqu'au jour de l'audience et ne peut donc préparer adéquatement son dossier.

Par contre, si les renseignements médicaux avaient été communiqués à l'employeur au moment où la plainte a été formulée, l'employeur qui serait au courant des preuves spécifiques du mauvais état de santé d'un employé s'efforcerait sans doute de régler rapidement le problème, évitant aux deux parties les délais et les frais d'une audience inutile.

Il existe un conflit évident entre l'obligation d'un médecin de compagnie envers son employeur et son devoir statutaire envers les personnes qui font appel à ses services professionnels.

La Commission Krever sur la Confidentialité des renseignements médicaux s'est penché sur ce problème dans son rapport.

Elle recommandait qu'on adopte une législation afin "de préciser clairement que l'obligation de confidentialité d'un employé membre d'une profession libérale a préséance sur son obligation d'obéir aux instructions de son employeur, lorsque celles-ci l'obligent à révéler des renseignements obtenus à titre confidentiel."⁶

La décision rendue en 1980 par une cour ontarienne au sujet du Dr Morton Shulman confirme qu'un médecin ne doit pas communiquer de renseignements sur son patient, quand bien même cette divulgation serait très utile sur le plan social.⁷

Nous pouvons tous imaginer des situations où l'impératif de la protection de la vie privée doit céder le pas à la nécessité d'une divulgation dans l'intérêt public. C'est la situation qui se présente lorsqu'un médecin de compagnie estime qu'un employé mettrait en danger sa santé ou sa sécurité, ou celles de ses compagnons de travail, s'il continuait à exécuter les tâches qui lui sont assignées.

On peut penser à l'exemple d'un employé affecté à l'assemblage d'automobiles et qui est sujet à des étourdissements. L'article 15 de la Loi sur la santé et la sécurité au travail de l'Ontario oblige les employeurs à "prendre toutes les précautions raisonnables dans les circonstances pour la protection d'un travailleur".

Un autre exemple serait celui d'un médecin de compagnie qui réalise que le taux de concentration en plomb dans le sang de certains employés dépasse les limites permises, donnant ainsi à penser que ces employés sont exposés à des concentrations de plomb élevées. Le médecin a le droit d'informer la direction de l'établissement que les niveaux de plomb sont trop élevés dans l'usine, mais il ne peut révéler l'identité des employés affectés. La direction est donc incapable de prendre des mesures efficaces pour remédier à une situation potentiellement dangereuse dans l'usine.

Pour que les employeurs puissent s'acquitter adéquatement de leur obligation de protéger les travailleurs sur les lieux de l'emploi aux termes de la Loi sur la santé et la sécurité au travail, ils ont besoin de renseignements spécifiques sur les risques de santé ou de sécurité, y compris les renseignements médicaux au sujet des employés concernés.

Il est évident qu'il serait nécessaire et souhaitable de modifier la Loi sur les professions médicales et paramédicales afin de permettre la communication de certains renseignements médicaux dans ce genre de situation.

2. La surveillance

Les compagnies incapables d'obtenir des preuves médicales avant une audience devraient-elles exercer une surveillance sur leurs employés afin de se procurer les renseignements nécessaires? La question se pose avec une acuité particulière dans les cas d'indemnisation pour accident du travail où l'employeur sait, ou soupçonne fortement, que l'employé est un simulateur, mais ne peut en faire la preuve par d'autres moyens.

Des photos ou des bandes magnétoscopiques des activités de l'employé présentées en preuve peuvent empêcher une personne non admissible à des prestations de les percevoir. Le juge ou le tribunal doit statuer sur la recevabilité d'une telle preuve.

La surveillance d'un employé à son insu a évidemment des conséquences sur sa vie privée. Toutefois le droit pénal ne semble pas interdire ce genre d'activités dans la mesure où elles ne s'accompagnent pas d'intrusion ou d'intimidation.

Comme nous l'avons mentionné, plusieurs provinces canadiennes ont adopté une législation sur la protection des renseignements personnels, prévoyant qu'une atteinte injustifiée à la vie privée d'une personne constitue un délit. Les lois de la Saskatchewan et de Terre-Neuve prévoient expressément que la surveillance auditive ou visuelle d'une personne, par quelque moyen que ce soit, constitue à priori une atteinte à la vie privée, qu'elle s'accompagne ou non d'une intrusion.

Personne ne saurait se dire en désaccord avec l'esprit de cette législation visant à protéger les citoyens contre les atteintes injustifiées à leur vie privée, mais elle peut paralyser une compagnie dont un des employés abuse du système et perçoit des prestations d'accidents du travail auxquelles il n'a pas droit.

3. Dossiers personnels - Collecte, stockage et
distribution des renseignements sur les employés

Les employeurs recueillent des renseignements permettant d'identifier les employés et ce, pour diverses raisons dans le cours de leurs affaires, comme l'administration des conventions collectives, des programmes d'avantages sociaux et autres motifs reliés à leurs activités, ou pour se conformer à divers lois et règlements fédéraux et provinciaux. Les renseignements personnels identifiables comprennent tous les renseignements pouvant être reliés à un employé, tel un nom, un numéro d'employé ou un numéro d'assurance sociale.

Il n'y a aucun doute qu'on a mis un plus grand accent, au sein des sociétés, sur le traitement équitable des dossiers des employés, leur confidentialité, leur exactitude et leur pertinence.

Des pratiques équitables d'information et une réelle préoccupation pour la protection des renseignements personnels sur les employés nous apparaissent compatibles avec une saine pratique commerciale.

J'ai pu constater par expérience que les sociétés importantes ont des procédures ou "codes de conduite" comprenant la plupart des lignes directrices suivantes, pour la protection des renseignements sur les employés:

1. Collecte et utilisation des données

On ne devrait recueillir que les renseignements pertinents et nécessaires pour la relation d'emploi. On ne devrait pas constituer ou maintenir de registres concernant les activités politiques d'un employé, sa participation à des associations, ses publications ou ses activités extra-professionnelles sans son autorisation écrite.

L'accès aux renseignements personnels sur un employé devrait être limité aux personnes qui ont légitimement besoin de ces renseignements dans la compagnie pour accomplir leurs tâches. On devrait aviser le personnel qui utilise ces renseignements qu'il est important d'assurer la confidentialité des renseignements personnels sur les employés.

Toutes les notes et lettres provenant de la direction contenues dans les dossiers personnels devraient être rédigées de façon claire et objective.

2. Communication des renseignements à l'extérieur de la compagnie

Les renseignements personnels sur les employés ne devraient pas être communiqués à l'extérieur de la compagnie sans le consentement écrit de l'employé, à moins d'y être obligé par la loi ou par ordre d'un tribunal.

Ce besoin de restreindre la communication de renseignements à des tiers devient d'autant plus apparent dans la mesure où les compagnies sont de plus en plus perçues comme des sources d'information par les parties à un litige, ou par celles qui envisagent d'intenter des poursuites.

Les demandes de renseignements portent notamment sur les points suivants:

- a) résumé du dossier professionnel d'un employé;
- b) périodes d'absence antérieure;
- c) disponibilité à effectuer des heures supplémentaires;
- d) exigences physiques pour un travail donné;
- e) coordonnées d'une personne;
- f) renseignements médicaux personnels;
- g) salaire et augmentations de salaire prévues.

Ces renseignements ne devraient pas être communiqués sans le consentement de l'employé concerné.

On peut penser à une situation typique, où un conjoint, qui a intenté des procédures devant un tribunal de la famille, demande des renseignements au sujet du revenu d'un employé. Cette demande est rejetée conformément aux lignes directrices de la compagnie et le conjoint demande alors la production des registres par voie d'assignation. On peut alors déboucher sur une situation où les administrateurs du personnel d'une compagnie passent presque autant de temps en cour qu'au bureau. Lorsque la demande vise des renseignements médicaux, l'administrateur du personnel n'aura pas le dossier médical, de telle sorte qu'une compagnie peut se retrouver avec deux employés en cour, l'administrateur du personnel et le médecin de la compagnie.

Une législation accordant aux employeurs une compensation raisonnable pour le temps et les frais consacrés à ces demandes de renseignements permettrait de réduire ces coûts et contribuerait à éliminer les demandes inutiles.

3. Consultation des dossiers personnels par les employés

Les compagnies font l'objet de pressions croissantes afin de donner aux employés le droit de consulter leur dossier personnel, ce qui est perçu comme un corollaire du droit à la protection des renseignements personnels contenus dans les dossiers. La Loi sur la protection des renseignements personnels fédérale contient des dispositions permettant aux individus d'avoir accès aux renseignements personnels détenus à leur sujet par une institution du gouvernement fédéral. Récemment, un projet de loi privé a été présenté devant la législature de l'Ontario, en vue de modifier

la Loi sur les normes d'emploi, afin de donner aux employés ontariens un droit d'accès aux renseignements personnels détenus par leur employeur à leur sujet.⁸

Je pense que la plupart des gens d'affaires appuient le principe voulant que les employés devraient avoir accès à leur dossier personnel. J'ai pu constater par expérience que les employés exercent rarement ce droit, puisque la plupart des compagnies font maintenant part à leurs employés de leur évaluation de rendement, au cours du processus d'évaluation.

4. Protection des renseignements techniques confidentiels des fournisseurs

La communication de renseignements techniques par un propriétaire à l'utilisateur de ces renseignements est une pratique courante dans l'univers commercial spécialisé, marqué par la haute technologie, des années 80. Les grandes multinationales diversifiées utilisent la technologie développée par d'autres entreprises spécialisées dans le domaine de la propriété intellectuelle. Cette propriété peut revêtir la forme de logiciels d'ordinateur, de plans et de dessins, de vidéocassettes, de cassettes de magnétophone, et ainsi de suite. Le fournisseur désire donc tout naturellement empêcher que ces renseignements techniques, qui constituent parfois son seul actif important, ne soient divulgués au public.

Afin de protéger leurs droits de propriété, les fournisseurs de renseignements se tournent vers la législation sur les brevets, les marques de commerce, les droits d'auteur et les dessins industriels, mais la plupart d'entre eux jugent ces lois inefficaces ou inadéquates pour protéger leurs précieux renseignements.

Par conséquent, les fournisseurs tentent de plus en plus d'obtenir une protection contractuelle pour leurs renseignements confidentiels, par le biais d'ententes de confidentialité. Ces ententes permettent aux fournisseurs d'imposer des obligations très sévères à la personne qui reçoit les renseignements. Les compagnies qui se trouvent dans ce genre de situation devraient faire preuve de prudence lorsqu'elles signent des ententes de confidentialité.

Ces ententes ne devraient couvrir qu'une période limitée, ne devraient viser que les communications écrites et devraient définir la norme de prudence dont doit faire preuve la compagnie qui reçoit les renseignements. Par exemple, cette dernière pourrait convenir d'assurer à ces renseignements la même protection qu'elle accorde à ses propres renseignements confidentiels.

Le Système de renseignements sur les produits dangereux en milieu de travail canadien (Canadian Workplace Hazardous Materials Information System) représente un phénomène nouveau en matière de protection des secrets industriels des fournisseurs et des renseignements confidentiels. L'industrie, les syndicats et le gouvernement ont élaboré un système qui permet aux fournisseurs de produits dangereux de donner à leurs utilisateurs des renseignements au sujet de ces produits, tout en

protégeant leurs secrets industriels. Les utilisateurs ont besoin de ces renseignements pour enseigner à leurs employés comment utiliser en toute sécurité ces produits dangereux sur les lieux de travail.

La mise en oeuvre de ce système permettra d'atteindre un équilibre entre ces deux besoins contradictoires: la communication des renseignements à l'utilisateur afin qu'il puisse former ses employés et la protection vitale des secrets industriels du fournisseur.

5. La confidentialité des renseignements commerciaux

Tout comme les individus se préoccupent de la confidentialité de leurs dossiers personnels, les compagnies prennent de grandes précautions afin d'empêcher que leurs renseignements commerciaux confidentiels ne soient divulgués à leurs concurrents et au public.

Comme beaucoup d'entre vous le savez déjà, la Loi sur l'accès à l'information fédérale est entrée en vigueur le 1^{er} juillet 1983. Cette législation, qui a pour objectif louable de promouvoir un gouvernement transparent et responsable, a fait l'objet d'un examen attentif de la part du secteur privé dont les dossiers confidentiels, qui sont en la possession d'agences gouvernementales, sont maintenant sujet à un examen public.

Plusieurs gouvernements provinciaux ont adopté ou, comme l'Ontario, envisagent d'adopter une législation semblable permettant au public d'avoir accès aux dossiers du gouvernement provincial.

Les dix mois d'application de la LAI indiquent que les compagnies sont devenues, ou devraient devenir, plus prudentes dans leurs relations avec le gouvernement fédéral, de crainte que des renseignements confidentiels ne soient divulgués au public. Les relations avec le gouvernement qui étaient autrefois moins formelles sont devenues plus rigides; les deux parties exigent que les demandes de renseignements soient faites par écrit; les réponses sont examinées avec soin et l'on s'applique à apposer le sceau "confidentiel" sur les documents. L'échange de renseignements entre le milieu des affaires et le gouvernement est maintenant régi par des lignes directrices rigides.

La récente décision de la Cour fédérale du Canada dans l'affaire Maislin Transport donne à penser que les inquiétudes du secteur privé sont bien fondées. Il est difficile d'apprécier exactement l'importance de cette décision, puisque nous ne connaissons pas les renseignements financiers spécifiques qui avaient un caractère confidentiel selon la compagnie Maislin, et qui ne devaient donc pas être communiqués.

Toutefois, il ressort clairement de cette décision "qu'il n'est pas suffisant que Maislin traite ces renseignements de façon confidentielle, mais ils doivent être en fait confidentiels selon une norme objective quelconque."

La cour semble appliquer le critère de la norme objective retenue dans l'affaire U.S. National Parks vs. Morten, où il a été décidé que, pour justifier la non-divulgence des renseignements, ceux-ci "doivent causer un préjudice substantiel à la position concurrentielle de la personne qui les a fournis."

Un critique américain a déclaré que le critère du préjudice substantiel causé à la position concurrentielle impose un fardeau de preuve presque insurmontable au demandeur. Par ailleurs, les efforts qu'il faut déployer pour recueillir la preuve nécessaire à prévenir la divulgation de documents sont si coûteux, que seules les plus grandes compagnies peuvent se les permettre.⁹

Il est à souhaiter, si l'Ontario adopte une loi sur la liberté de l'information, qu'elle n'imposera pas des normes de divulgation si sévères qu'elles dissuadent les compagnies de communiquer en toute liberté avec leur gouvernement, de crainte que leurs renseignements confidentiels ne soient divulgués.

Conclusion

L'existence du matériel électronique perfectionné utilisé de nos jours dans les affaires permet de recueillir, de réunir et de distribuer l'information rapidement et à plusieurs destinataires. Cette faculté est essentielle pour rester concurrentiel dans l'économie globale contemporaine. Nous devons assurer le respect des intérêts de toutes les parties concernées - atteindre cet équilibre délicat qui protégera les droits de toutes les parties, tout en permettant d'utiliser la ressource la plus précieuse de la société: l'information. C'est le défi posé aujourd'hui au gouvernement et au monde des affaires.

R.W. McFarlane, c.r.

23 mai 1984

NOTES

1. Hugh Rowan, Q.C., "Privacy and the Law", Law Society of Upper Canada Special Lectures, 1973, pp. 259-307.
2. Peter Burns, "The Law and Privacy: The Canadian Experience", (1976), 54 Canadian Bar Review 1.
3. R. Dale Gibson, "Legal Protections of Privacy", The Practice of Freedom, Canadian Essays on Human Rights and Fundamental Freedoms, 1979.
4. Coderque v Mutual of Omaha Insurance Co., [1970] 1 O.R. 473 (Cour Suprême de l'Ontario)
5. Règlement sur les disciplines de la santé, R.R.O. 1980, Règ. 448, par. 27(22).
6. Report of the Commission of Inquiry into the Confidentiality of Health Information, volume III, pp. 167-168.
7. Re Shulman and College of Physicians & Surgeons of Ontario (1980), 29 OR (2d) 40 (Cour Divisionnaire de l'Ontario).
8. Projet de loi 20 - Loi modifiant la Loi sur les normes d'emploi (Reid, Rainy River).
9. Jack I. Pulley, Senior Environment Attorney, Dow Corning Corporation, "The Freedom of Information Act - A Government Subsidy for Industrial Espionage." p. 11

INTERPROVINCIAL CONFERENCE ON PRIVACY:
INITIATIVES FOR 1984 (SYMPOSIUM)

Presentation

By

Dr. W. Ghent
Chairman of the
Council on Health Care for the
Canadian Medical Association

Toronto, Ontario
May 23-24, 1984

DR W. G. HENT

CONFERENCE ON PRIVACY
INITIATIVES FOR 1984

Toronto - May 23

I must state at the outset that I am not the official spokesman for the Canadian Medical Association on this subject. I am the Chairman of the Council on Health Care for the Canadian Medical Association and as such, we are in the process of formulating some guidelines on this subject. *present topic by the medical profession*

It has been considered¹ in the past, that our Code of Ethics covered this subject adequately for the protection of the individual patient's rights of privacy and confidentiality.

The medical Code of Ethics that has guided ~~the medical profession~~ ^{us} for hundreds of years, was first formalized by Hippocrates, who wrote, "All that may come to my knowledge in the exercise of my profession or outside my profession or in daily commerce with men, which ought not to be spread abroad, I will keep secret and will never reveal". Succinctly reproduced as Article IV in the C.M.A. Code of Ethics, this principle is stated "Protect the patient's secrets".

Legally the principle of patient confidentiality has been documented in Regulation 448, Section 22, of the Health Disciplines Act of Ontario, "giving information concerning the patient's condition, or any professional services performed for a patient to any person other than the patient without the consent of the patient unless required to do so by law"; is considered to be an act of misconduct by the medical profession. I would like to emphasize the last statement as of importance, "unless required to do so by law"; and return to this later.

The consent procedural guidelines are waived by the medical profession in the case of Life Insurance Companies and Proof of Death certificates, necessary to provide the insurer the grounds for payment of death benefits to the family of the insuree. This is understandable and acceptable, both socially and medically. As a conclusion to the "need to know" group, it is a *Sin e qua non* that the patient is the first to know and the immediate family are of next importance in cases where the patient is unable to transmit personal information.

We now enter a grey zone of legal requirements of the "need to know", "would know" variety or "unless required to do so by law". I will state categorically at the outset that governmental agencies are the most blatant and most pernicious purveyors of the erosion of privacy in the health care field.

There are many examples of this slow invasion of privacy by bureaucrats. This first began with the compulsory notification of communicable diseases, without the patient's permission, and with the advertisement of the disease placarded on the front door of the patient so inflicted. I can still remember the "Measles" sign that decorated our front door when I was a kid. This practice has been abandoned by medical advances but not due to public clamour, unfortunately.


The same communicable disease Statutes still apply to the "social diseases" of our society, and the notification on occasion can have tragic results. However, more and more of the medical profession disregard this law as inappropriate, if not stupid, circa 1984.

Another example of government "would know" by Statute concerns

patients whom a doctor considers medically unfit to drive. The doctor is required, under penalty of law, to notify the Motor Vehicles Branch of this patient, with his diagnosis, and without his consent.

The loss of privacy by governmental decree is most worrisome as Ontario Hospital Insurance Plan and its computers obtain, without permission, the diagnosis and treatment afforded each resident of Ontario who seeks medical aid under the plan. This is an OHIP card, the billing mechanism employed by doctors, on behalf of their patients, to receive payment for their services. It contains name, OHIP number, address, date of birth, sex, diagnosis, treatment and date services rendered. This is signed by the doctor. The average patient has no idea of the personal data that has been transmitted to a government agency, and, certainly, the patient has not personally, actively authorized this release of information. This is made legal by the following quote from the Health Insurance Act: Section 33-2:

Every insured person shall have been deemed to have authorized his physician or practitioner who performed insured services to provide the General Manager with such information respecting insured services performed as the General Manager requires for the purposes of the plan. ** - had law - named person to whom information may be transmitted*

I suppose the legal jargon, a "Notwithstanding Section 448, Subsection 22 of the Health Disciplines Act" should be added. 

It is interesting to follow one of these information packages from a medical office to its ultimate destination in the great white computer in Kingston.

At least five secretarial staff have access to these cards before they reach the computer. Once computerized, the information is stored for sixty days in the computer, and then it is microfilmed for ongoing storage.

I am assured by OHIP that their files and systems are secure except for a court order release. However, the integrity of the storage system must be questioned in view of the recent computer break-ins by educated High School students. This is, of course, the theme of this conference, and as a member of the medical community, I would like to wish you all success. As far as we are concerned, the interest is long overdue.

The public, by and large, are unaware of the governmental health file that is being compiled about them, and I would think this represents the greatest hazard to public privacy that has ever existed in recorded time. We can be assured by the Ministry of Health that all is well and all is secure, but in all honesty, it must be questioned.

The "would knows" of this world are still with us medically, such as the neighbour who contacts the surgeon to find out what was done to his or her "closest friend". Then of course, the ridiculous state of affairs that arise when there are 13 kids and none of them talk to each other or to their parents. The permutations and combinations of queries about who did what to dear Mother and when, are limitless and irrevocably unanswerable except by next of kin.

There could be a more sinister and sophisticated "would know" group on the horizon - a group of experts who, for a price, will steal from

personal health file of OHIP for pre-employment information, blackmail, etc.

The Federal Government has never been noted for its sensitivity to privacy or confidentiality - except for its own ends. The latest example of potential invasion of privacy by search and seizure is contained in Bill C9 - our Security Force Act. At least four clauses in this Bill allow for search of any premises for any information, including medical

upon suspicion. *of security breach. The comments she has allowed C.M.A. official to make.*

Of more immediate concern to the medical profession, is the invasion of patient's privacy to be allowed with Bill C123. This Bill is to establish an investigative protocol for aircraft accidents. One clause would provide an investigator, not a medical person, *He legal leave* to examine a doctor's medical files of any person who may have had contact with a pilot involved in an air crash.

In conclusion, the medical profession has kept faith with the public; the private insurance carriers have kept faith with the public. The offender, by and large, is the bureaucracy of government - provincial and federal. Formally, I would warn each and every resident of Ontario and of Canada that the confidentiality of your health status is in jeopardy.

CA1
Z4
-C62

DOCUMENT : 870-123/014

Traduction du Secrétariat

CONFÉRENCE INTERPROVINCIAL SUR LA PROTECTION DES
RENSEIGNEMENTS PERSONNELS :
MESURE POUR 1984 (COLLOQUE)

Allocution

par

le docteur W. Ghent
Président du
Conseil des soins de santé de
l'Association médicale canadienne



Toronto (Ontario)
Les 23 et 24 mai 1984

CONFÉRENCE SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

MESURES POUR 1984

Toronto - le 23 mai

Je dois d'abord dire que je ne suis pas le porte-parole officiel de l'Association médicale canadienne sur cette question. Je suis président du Conseil des soins de santé de l'Association et nous rédigeons actuellement des lignes directrices touchant ce point.

Dans le passé, la profession médicale a toujours cru que notre code de déontologie couvrirait de façon adéquate la question de la protection des droits individuels du malade à la vie privée et à la protection des renseignements personnels le concernant.

Le code de déontologie qui nous guide depuis des centaines d'années a d'abord été exprimé par Hippocrate qui écrivait : "Les choses que, dans l'exercice ou même hors de l'exercice de mon art, je pourrai voir ou entendre sur l'existence des hommes et qui ne doivent pas être divulguées au dehors, je les tairai, estimant que ces choses-là ont droit au secret des Mystères." Retranscrit de façon succincte à l'article IV du Code de déontologie de l'Association, ce principe se lit comme suit : "Protéger les secrets du malade".

Le principe de la protection des renseignements sur les malades est inscrit à l'article 22 du règlement de la Loi sur les professions médicales et paramédicales de l'Ontario. En effet, donner des renseignements sur la condition du malade, ou tous services professionnels rendus à un malade ou à toute autre personne, sans le consentement du malade, à moins que cette divulgation ne soit exigée par la loi, est considéré comme un acte de mauvaise conduite par la profession médicale. J'aimerais souligner la dernier élément de cet énoncé "à moins que cette divulgation ne soit exigée par la loi" comme étant importante, et j'y reviendrai plus tard.

La profession médicale déroge aux lignes directrices relatives au consentement dans le cas des compagnies d'assurance-vie et des certificats de décès qui sont nécessaires pour permettre le versement des prestations de décès à la famille de l'assuré. Cette dérogation est compréhensible et acceptable du point de vue tant social que médical. Pour ce qui est du groupe de ceux qui ont "besoin de savoir", il va sans dire que le malade est la première personne qui a besoin de savoir et que les membres de la famille immédiate viennent ensuite lorsque le malade ne peut transmettre lui-même les renseignements personnels.

Nous entrons maintenant dans une zone grise d'exigences juridiques touchant ceux qui ont "besoin de savoir", ceux qui "veulent savoir" ou les cas prévus par l'expression "à moins que cette divulgation ne soit par la loi". Tout d'abord, je voudrais affirmer catégoriquement que les organismes gouvernementaux sont ceux qui contribuent de la façon la plus flagrante et la plus pernicieuse à l'érosion de la protection des renseignements personnels dans le domaine de la santé.

On pourrait citer de nombreux exemples de cette lente invasion de la vie privée par les bureaucrates qui a commencé par l'obligation de signaler les maladies transmissibles, sans la permission du malade, et d'apposer une affiche à la porte d'entrée où une telle maladie sévissait. Je me souviens toujours du signe "rougeole" qui a décoré notre porte d'entrée lorsque j'étais enfant. Cette pratique a été abolie grâce au progrès de la médecine mais non, malheureusement, à la suite de revendications du public.

Les mêmes règles s'appliquent toujours aux "maladies sociales" de notre société, et le fait de les signaler peut parfois avoir des conséquences tragiques. Toutefois, de plus de plus de membres de la profession médicale passent outre à cette loi qu'ils considèrent inopportune, sinon stupide, à notre époque.

Un autre exemple de la nécessité de transmettre des renseignements aux gouvernements en vertu d'une loi touche les malades qu'un médecin considère inapte à conduire. Celui-ci est obligé, par la loi, de signaler ce patient, sans son consentement, au bureau des véhicules moteurs et de faire connaître son diagnostic.

Les atteintes à la vie privée prévues par décret gouvernemental sont très inquiétantes, car le Régime d'assurance-maladie de l'Ontario peut, à l'aide de ses ordinateurs, obtenir, sans permission, le diagnostic et le traitement fournis à tout résident de l'Ontario qui demande de l'aide médicale en vertu du régime. Ces renseignements sont obtenus grâce à la fiche dont les médecins se servent pour se faire rembourser les frais des services rendus aux malades. Cette fiche renferme le nom, le numéro de l'OHIP, l'adresse, la date de naissance, le sexe, le diagnostic, le traitement subi et la date des services rendus, et elle est signée par le médecin. Le patient moyen n'a aucune idée des renseignements personnels qui ont été transmis à un organisme gouvernemental et, cela va sans dire, il n'a pas personnellement autorisé cette divulgation qui est légale en vertu de l'article 33-2 de la Loi sur l'assurance-maladie qui se lit ainsi :

Chaque assuré est réputé avoir autorisé le médecin ou praticien qui lui a fourni les services assurés à divulguer

à l'administration général les renseignements à l'égard de ces services et que celui-ci exige aux fins du régime.

Je suppose qu'il aurait fallu ajouter, dans le jargon juridique, "Par dérogation au paragraphe 448(22) de Loi sur les professions médicales et paramédicales" si la loi avait nommé une personne à qui les renseignements pouvaient être transmis.

Il serait intéressant de suivre ces renseignements d'un bureau de médecin jusqu'à sa destination finale dans le grand ordinateur de Kingston.

Au moins cinq membres du personnel de soutien ont accès à ces fichiers avant qu'ils ne soient inscrits dans l'ordinateur. Une fois informatisés, les renseignements sont stockés pendant soixante jours dans l'ordinateur et sont ensuite transcrits sur microfilm.

On m'assure que les fichiers et les systèmes de l'OHIP sont gardés en lieu sûr et ne sont divulgués qu'à la suite d'une ordonnance d'un tribunal. Toutefois, on peut douter de la sécurité des systèmes de stockage quant on constate que des élèves brillants d'écoles secondaires peuvent déjouer les ordinateurs. Ce danger constitue le thème de la présente conférence et, comme membre du monde médical, je voudrais vous souhaiter tout le succès possible. Quant à nous, nous croyons que l'étude de cette question se fait attendre depuis longtemps.

Dans l'ensemble, le public n'est pas au courant des fichiers de santé que les gouvernements compilent à son sujet, et je crois que cette compilation constitue la plus grave atteinte à la vie privée qui n'a jamais existé. Les ministères de la Santé peuvent nous assurer que tous les renseignements sont gardés dans des endroits sûrs, mais, en toute honnêteté, nous en doutons.

Ceux qui "veulent savoir" nous entourent toujours, par exemple le voisin qui communique avec le chirurgien afin de savoir ce qui est arrivé à son "meilleur ami". Il y a aussi la situation ridicule de la famille de treize enfants qui ne se parlent pas entre eux et qui ne parlent pas à leurs parents. Il en découle un chassé-croisé de questions concernant la condition de la mère, les traitements qu'elle a reçus, par qui et quand, questions auxquelles seul le plus proche parent peut répondre.

L'avenir pourrait voir apparaître un groupe plus menaçant et plus spécialisé de personnes qui "veulent savoir", c'est-à-dire un groupe d'experts qui, moyennant rémunération, pourraient voler des dossiers de renseignements personnels de l'OHIP dans des cas de demandes d'emploi, pour faire du chantage, etc.

Le gouvernement fédéral n'a jamais été reconnu comme étant très sensible à la protection des renseignements personnels, sauf pour ses propres besoins. L'exemple le plus récent de possibilité d'atteinte à la vie privée au moyen de perquisition figure au projet de loi C-9, la loi sur le service de sécurité. Au moins quatre dispositions de ce projet de loi permettent la perquisition de n'importe quel lieu, pour obtenir des renseignements, y compris des renseignements médicaux, si l'on soupçonne qu'il y a eu atteinte à la sécurité. L'Association médicale canadienne a officiellement fait connaître ses préoccupations à ce sujet à la Chambre des communes.

Une question qui préoccupe d'une façon plus immédiate la profession médicale est celle de l'atteinte à la vie privée que prévoit le projet de loi C-123. Ce projet vise à établir un protocole d'enquête à la suite d'accidents d'avion. En vertu d'une des dispositions, un enquêteur, qui ne fait pas partie du personnel médical, pourrait examiner les dossiers d'un médecin concernant toute personne qui est entrée en rapport avec un pilote impliqué dans un accident d'avion.

Pour conclure, j'ajouterai que la profession médicale a tenu ses promesses envers le public et que les compagnies d'assurance privées ont fait de même. Généralement parlant, le coupable est la bureaucratie gouvernementale, au niveau tant provincial que fédéral. J'aimerais avertir officiellement chaque résident de l'Ontario et du Canada que la protection des renseignements concernant sa santé est menacée.

CA1
Z4
C52

INTERPROVINCIAL CONFERENCE ON PRIVACY:
INITIATIVES FOR 1984 (SYMPOSIUM)

Presentation

By

Eric Wimberley
Vice-President
Association Affairs
Canadian Cable Television Association



Toronto, Ontario
May 23-24, 1984

CONFERENCE ON PRIVACY - MAY 23, 1984 - TORONTO

GOOD AFTERNOON LADIES AND GENTLEMEN. MY NAME IS ERIC WIMBERLEY AND I AM VICE-PRESIDENT ASSOCIATION AFFAIRS FOR THE CANADIAN CABLE TELEVISION ASSOCIATION. OUR ASSOCIATION WAS FORMED BACK IN 1957 BY A GROUP OF ENTREPRENEURIAL CABLE OPERATORS WHO RECOGNIZED THE NEED EVEN AT THAT EARLY STAGE FOR SOME SORT OF COORDINATION IN THE DEVELOPMENT OF AN INDUSTRY WHICH AT THAT TIME REPRESENTED ONLY SMALL POCKETS OF THE POPULATION MAINLY IN THE URBAN AREAS OF CANADA. TODAY THE CABLE INDUSTRY HAS GROWN TO COVER MORE THAN 60% OF THE CANADIAN POPULATION. THE CCTA NOW REPRESENTS SOME 380 CABLE LICENSEES FROM NEWFOUNDLAND TO VANCOUVER ISLAND WHO IN TURN SERVE SOME 4.8 MILLION SUBSCRIBERS OR APPROXIMATELY 95% OF ALL CANADIANS WHO RECEIVE TELEVISION VIA CABLE.

BACKGROUND

USING A SOPHISTICATED ANTENNA SYSTEM, THE CABLE OPERATOR IS ABLE TO OFFER HIS SUBSCRIBERS SIGNALS WHICH WOULD NOT OTHERWISE BE AVAILABLE TO THEM. UNTIL A FEW YEARS AGO A TYPICAL SYSTEM HOWEVER STILL CONSISTED OF THE BASIC TWELVE CHANNELS LOCATED IN THE VHF BAND. TODAY, 35 CHANNEL SYSTEMS ARE CONSIDERED MORE OR LESS NORMAL IN CANADA, AND 54 CHANNEL SYSTEMS ARE NOT FAR AWAY. IN THE UNITED STATES, WHERE THE REGULATORY ENVIRONMENT IS CONSIDERABLY DIFFERENT TO CANADA, 108 CHANNEL SYSTEMS EXIST.

THE VARIETY OF SERVICES WHICH CAN NOW BE OFFERED TO A SUBSCRIBER BY THE TELEVISION SYSTEM IS ONE REASON WE ARE HERE TODAY. UNTIL VERY RECENTLY EVERY CABLE SUBSCRIBER TO THE SYSTEM RECEIVED THE SAME SIGNALS. A CABLE WAS INSTALLED FROM THE TRUNK LINE ON THE STREET TO THE SUBSCRIBER'S TV SET AND THE COMPLETE RANGE OF SIGNALS OFFERED BY THAT PARTICULAR CABLE COMPANY WAS BROUGHT INTO THE HOME.

DISCRETIONARY

SERVICES

HOWEVER, WITH THE ADVENT OF PAY TV JUST OVER A YEAR AGO, CABLE OPERATORS WERE ABLE TO OFFER THEIR SUBSCRIBERS A NUMBER OF DISCRETIONARY SERVICES, DISCRETIONARY IN THAT THE SUBSCRIBER CAN CHOOSE TO RECEIVE THE ADDITIONAL SERVICE OR NOT, OR IN FACT TO RECEIVE ONLY A PORTION OF THE ADDITIONAL SERVICE. THIS FACT HAS LED TO THE REQUIREMENT FOR A DEVICE IN THE HOME WHICH MOST PEOPLE KNOW AS A DECODER BUT WHICH IS MORE PROPERLY TERMED A HOME TERMINAL UNIT. THIS UNIT ENABLES THE CABLE OPERATOR TO ADDRESS EACH INDIVIDUAL SUBSCRIBER TO HIS SYSTEM DIRECTLY FROM THE CABLE COMPANY OFFICE AND TO OFFER EACH INDIVIDUAL SUBSCRIBER THE PARTICULAR DISCRETIONARY SERVICES WHICH THAT SUBSCRIBER WISHES TO RECEIVE. OBVIOUSLY THE COST OF THE SERVICE TO A PARTICULAR SUBSCRIBER WILL DEPEND TO A DEGREE UPON THE SERVICES TO WHICH HE CHOOSES TO SUBSCRIBE.

IN ORDER TO PROVIDE ADEQUATE SERVICE AND TO PROPERLY BILL THE CUSTOMER, THE CABLE OPERATOR MUST OF NECESSITY KNOW JUST WHAT SERVICES THAT SUBSCRIBER IS RECEIVING. THE SIMPLE RECORDING OF THIS INFORMATION SHOULD NOT IN ITSELF BE CONSIDERED A THREAT TO THE SUBSCRIBER'S PRIVACY. IT IS SIMPLY THE RECORDING OF INFORMATION NECESSARY FOR BILLING PURPOSES, SIMILAR TO THAT RECORDED FOR EXAMPLE BY THE TELEPHONE COMPANIES IN RELATION TO LONG DISTANCE CHARGES.

SOMETIME IN THE FUTURE HOWEVER WE EXPECT TO PROVIDE TWO-WAY SERVICES TO OUR SUBSCRIBERS. THE SERVICE WILL BE PROVIDED AND THE INDIVIDUAL SUBSCRIBER'S RESPONSE TO THE SERVICE WILL BE RECEIVED IN THE CABLE COMPANY OFFICE. IT IS THE COLLECTION OF THIS INDIVIDUALIZED DATA WHICH HAS LED THE CABLE INDUSTRY TO REVIEW ITS POSITION AS TO ITS RESPONSIBILITIES REGARDING TREATMENT OF THAT DATA AND WHAT EFFECT THIS INFORMATION MIGHT HAVE ON THE PRIVACY RIGHTS OF A PARTICULAR SUBSCRIBER. ALTHOUGH A VERY FEW CABLE SYSTEMS ARE EXPERIMENTING WITH TWO-WAY SERVICES EVEN NOW, IN OUR OPINION IT WILL BE SOME TIME BEFORE THESE SERVICES BECOME WIDESPREAD. FORTUNATELY THIS PROVIDES TIME FOR US TO ASSESS THE SITUATION AND TO DEVELOP A WORKABLE CODE WHICH ADDRESSES THE INTERESTS OF BOTH THE CONSUMER AND THE INDUSTRY.

THE STUDY

EARLY IN 1983, IMMEDIATELY FOLLOWING THE INTRODUCTION OF THE FIRST DISCRETIONARY SERVICES, THE CABLE INDUSTRY, THROUGH ITS NATIONAL ASSOCIATION THE CCTA, INITIATED A STUDY INTO THE NECESSITY FOR A CODE OF PRIVACY FOR THE INDUSTRY. WE LOOKED FIRST TO OUR COUNTERPARTS IN THE UNITED STATES WHERE DISCRETIONARY SERVICES HAVE BEEN IN EXISTENCE FOR SOME YEARS. WE REVIEWED THE EXISTING CODES OF A NUMBER OF LARGE CABLE COMPANIES AND AMERICAN ASSOCIATIONS INCLUDING COX CABLE OF ATLANTA, GEORGIA, THE NEW JERSEY CABLE TELEVISION ASSOCIATION, THE NEW ENGLAND CABLE TELEVISION ASSOCIATION, THE VIDEOTEX INDUSTRY ASSOCIATION OF WASHINGTON, D.C. AND THE OFTEN MENTIONED WARNER AMEX CODE OF PRIVACY. IN ADDITION, THE PRIVACY CODE DEVELOPED INTERNALLY BY ROGERS CABLE, THE LARGEST CABLE OPERATOR IN CANADA WAS ALSO EXAMINED.

THROUGH THIS STUDY, WE HAVE DEVELOPED WHAT WE BELIEVE IS A PRIVACY CODE WHICH WILL ADEQUATELY PROTECT THE INTERESTS OF CABLE SUBSCRIBERS IN CANADA. EARLIER THIS YEAR IT WAS REVIEWED BY OUR BOARD OF DIRECTORS AND IT IN TURN HAS RECOMMENDED ACCEPTANCE BY THE NATIONAL ASSOCIATION MEMBERSHIP. THE PROPOSED CODE WILL BE DISCUSSED AT THE ANNUAL GENERAL MEETING SCHEDULED FOR THE SECOND WEEK OF JUNE IN OTTAWA AT WHICH TIME WE EXPECT IT WILL BE ACCEPTED BY THE GENERAL MEMBERSHIP OF THE ASSOCIATION.

CODE

WHILE I OBVIOUSLY AM NOT AT LIBERTY TO RELEASE THE PROPOSED CODE PENDING ACCEPTANCE BY THE MEMBERSHIP I CAN OUTLINE THE AREAS OF CONCERN WHICH IT ADDRESSES.

INFORMATION COLLECTION: -

THE CODE WILL REQUIRE THAT INDIVIDUAL SUBSCRIBERS BE MADE AWARE OF THE INFORMATION WHICH IS BEING COLLECTED AND THE REASONS FOR THE COLLECTION OF THAT INFORMATION. ONLY INFORMATION NECESSARY TO PERMIT BILLING OR TO PROVIDE ADEQUATE SERVICE TO THE SUBSCRIBER WILL BE COLLECTED AND WILL BE RETAINED ONLY AS LONG AS IS NECESSARY FOR BILLING OR SERVICING PURPOSES AND WILL THEN BE DESTROYED.

SECURITY: -

ALL REASONABLE STEPS WILL BE TAKEN TO ENSURE THE PHYSICAL SECURITY OF THE INFORMATION COLLECTED. ACCESS TO DATA COLLECTED WILL BE RESTRICTED TO EMPLOYEES WHO ARE DIRECTLY CONCERNED WITH THE OPERATION OF THE SERVICES INVOLVED.

SUBSCRIBER ACCESS: -

SUBSCRIBERS WILL BE ALLOWED REASONABLE ACCESS TO INFORMATION ON FILE AND THE RIGHT TO HAVE ERRONEOUS INFORMATION CORRECTED.

THIRD PARTY: -

ADHERENCE TO THE PRIVACY POLICY WILL BE REQUIRED OF ANY THIRD PARTIES WHO MAY PARTICIPATE IN PROVIDING SERVICES TO THE CABLE COMPANIES' SUBSCRIBERS.

LEGAL COMPLIANCE: -

INDIVIDUAL SUBSCRIBER INFORMATION WILL BE MADE AVAILABLE TO GOVERNMENT AGENCIES ONLY UNDER COURT ORDER OR OTHER LEGAL COMPULSION AND, UNLESS PROHIBITED BY LAW, SUBSCRIBERS WILL BE MADE AWARE OF ANY SUCH LEGAL REQUESTS FOR INFORMATION.

POLICY REVIEW: -

AND FINALLY SINCE OUR INDUSTRY IS SUBJECT TO VERY RAPID CHANGE, THERE MUST BE PROVISION FOR A REVIEW OF THE CODE OF PRIVACY, IN ORDER TO ENSURE THAT CURRENT LEGAL AND TECHNOLOGICAL DEVELOPMENTS ARE ADEQUATELY ADDRESSED.

INDUSTRY

POSITION

WE BELIEVE A VOLUNTARY CODE WILL ADEQUATELY ADDRESS PRIVACY REQUIREMENTS OF THE CABLE INDUSTRY AND WILL PROVIDE THE FLEXIBILITY WHICH IS NECESSARY FOR THE CABLE INDUSTRY TO

ADAPT TO THE RAPIDLY CHANGING ENVIRONMENT IN WHICH IT MUST OPERATE. WHILE CABLE IS VIEWED IN MANY QUARTERS AS A MONOPOLY, AND PERHAPS AT ONE TIME THIS WAS TRUE, SUCH IS NOT THE CASE TODAY. TODAY CABLE MUST COMPETE WITH A VARIETY OF OTHER SERVICES ALL VYING FOR THE SUBSCRIBER'S TIME AND DOLLAR INCLUDING LIVE THEATRE, MORE SOPHISTICATED HOME ANTENNAS, EARTH STATIONS WHICH CAN RECEIVE A WIDE VARIETY OF SATELLITE DELIVERED SERVICES AND OF COURSE THE RECENT EXPLOSION IN THE HOME VCR MARKET.

GOVERNMENT REGULATION IS NOT NEW TO OUR INDUSTRY. THE CANADIAN RADIO-TELEVISION AND TELECOMMUNICATIONS COMMISSION CLOSELY REGULATES WHAT A CABLE SYSTEM CAN AND CANNOT DO. HOWEVER EVEN THIS COMMISSION HAS RECOGNIZED THE NEED TO EASE THE REGULATORY LOAD WHEREVER POSSIBLE IN ORDER TO ALLOW THE CABLE INDUSTRY TO RESPOND ADEQUATELY TO THE INCREASINGLY COMPETITIVE ENVIRONMENT IN WHICH IT FINDS ITSELF. IN OUR VIEW, GOVERNMENT REGULATION, EITHER FEDERAL OR PROVINCIAL, OF A MATTER WHICH CAN ADEQUATELY BE ADDRESSED BY THE PRIVATE SECTOR WOULD BE PREMATURE.

OF COURSE THERE IS ANOTHER WAY. ONE WELL-KNOWN WRITER STATED THAT "IN ORDER TO AVOID INVASION OF PRIVACY, ONE NEED ONLY ARRANGE ONE'S AFFAIRS IN SUCH A BORING FASHION THAT NO ONE WISHES TO FIND OUT ABOUT YOU IN ANY CASE".

THANK YOU!

CA 1
Z 4
- C 52

DOCUMENT : 870-123/015
Traduction du Secrétariat

CONFÉRENCE INTERPROVINCIALE SUR LA PROTECTION
DES RENSEIGNEMENTS PERSONNELS :
MESURES POUR 1984 (COLLOQUE)

Exposé

de

Eric Wimberley
Vice-président
Affaires de l'Association
Association canadienne de télévision par câble



Toronto (Ontario)
Les 23 et 24 mai 1984

CONFÉRENCE SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

- LE 23 MAI 1984 - TORONTO

BON APRÈS-MIDI MESDAMES ET MESSIEURS. JE M'APPELLE ERIC WIMBERLEY ET JE SUIS VICE-PRÉSIDENT POUR LES AFFAIRES DE L'ASSOCIATION CANADIENNE DE TÉLÉVISION PAR CÂBLE. NOTRE ASSOCIATION FUT FONDÉE EN 1957 PAR UN GROUPE D'ENTREPRENEURS EN CÂBLODISTRIBUTION QUI SE RENDAIENT DÉJÀ COMPTE, À CE STADE PRÉCOCE, DE LA NÉCESSITÉ D'UNE COORDINATION QUELCONQUE DE L'ÉVOLUTION D'UNE INDUSTRIE QUI NE TOUCHAIT, À CE MOMENT-LÀ, QU'UNE INFIME PARTIE DE LA POPULATION DANS LES PRINCIPAUX CENTRES URBAINS DU CANADA. L'INDUSTRIE DE LA CÂBODISTRIBUTION A AUJOURD'HUI UNE AMPLEUR TELLE QU'ELLE REJOINT PLUS DE 60 p. 100 DE LA POPULATION CANADIENNE. L'ASSOCIATION CANADIENNE DE TÉLÉVISION PAR CÂBLE REPRÉSENTE MAINTENANT QUELQUE 380 TITULAIRES DE PERMIS DE CÂBLODISTRIBUTION DE TERRE-NEUVE À L'ÎLE DE VANCOUVER. CES TITULAIRES DESSERVENT ENVIRON 4,8 MILLIONS D'ABONNÉS OU APPROXIMATIVEMENT 95 p 100 DE TOUS LES CANADIENS QUI REÇOIVENT LA TÉLÉVISION PAR CÂBLE.

ÉTAT DE LA QUESTION

AU MOYEN D'UN SYSTÈME D'ANTENNES COMPLEXES, LE CÂBLODISTRIBUTEUR EST EN MESURE D'OFFRIR À SES ABONNÉS DES SIGNAUX QU'ILS NE PEUVENT CAPTER AUTREMENT. TOUTEFOIS, JUSQU'À IL Y A QUELQUES

ANNÉES, LE RÉSEAU TYPE NE COMPORTAIT QUE LES DOUZE CANAUX DE LA BANDE THF. DE NOS JOURS, LES RÉSEAUX À 35 CANAUX SONT PLUS OU MOINS COURANTS AU CANADA ET LE JOUR N'EST PAS LOIN OÙ L'ON POURRA OFFRIR DES RÉSEAUX À 54 CANAUX. AUX ÉTATS-UNIS, OÙ LA RÉGLEMENTATION EST TRÈS DIFFÉRENTE DE CE QU'ELLE EST AU CANADA, IL Y A DES RÉSEAUX DE 108 CANAUX. LA DIVERSITÉ DES SERVICES QU'UN RÉSEAU DE TÉLÉVISION PERMET MAINTENANT D'OFFRIR À UN ABONNÉ EST UNE DES RAISONS POUR LESQUELLES NOUS NOUS RÉUNISSEMS AUJOURD'HUI. JUSQU'À TOUT RÉCEMMENT, TOUS LES ABONNÉS DE TÉLÉDISTRIBUTION RECEVAIENT LES MÊMES SIGNAUX. UN CÂBLE ÉTAIT INSTALLÉ ENTRE LA CONDUITE PRINCIPALE SITUÉE DANS LA RUE ET L'APPAREIL DE L'ABONNÉ, CE QUI PERMETTAIT D'ACHEMINER AU FOYER DE CE DERNIER LA GAMME COMPLÈTE DE SIGNAUX OFFERTS PAR LA SOCIÉTÉ DE CÂBLODISTRIBUTION À LAQUELLE IL ÉTAIT ABONNÉ.

SERVICES

DISCRÉTIONNAIRES

TOUTEFOIS, AVEC L'ARRIVÉE DE LA TÉLÉVISION À PÉAGE IL Y A UN PEU PLUS D'UN AN, LES CÂBLODISTRIBUTEURS ONT PU OFFRIR À LEURS ABONNÉS UN CERTAIN NOMBRE DE SERVICES DISCRÉTIONNAIRES. CES SERVICES SONT DISCRÉTIONNAIRES PARCE QUE L'ABONNÉ A LE CHOIX DE RECEVOIR OU DE REFUSER EN TOUT OU EN PARTIE, LES SERVICES ADDITIONNELS. CE PHÉNOMÈNE A RENDU NÉCESSAIRE L'INSTALLATION AU FOYER D'UN DISPOSITIF COMMUNÉMENT APPELÉ DÉCODEUR MAIS QU'IL EST

PLUS EXACT DE DÉSIGNER COMME UN TERMINAL DOMESTQUE. CET ÉLÉMENT PERMET AU CÂBLODISTRIBUTEUR DE RACCORDER DIRECTEMENT CHAQUE ABONNÉ À SON RÉSEAU, AU BUREAU MÊME DE LA SOCIÉTÉ DE CÂBLO-DISTRIBUTION ET D'OFFRIR À CHAQUE ABONNÉ LES SERVICES DISCRÉTIONNAIRES PRÉCIS QUE CELUI-CI DÉSIRE OBTENIR. IL VA DE SOI QUE LES FRAIS QUE DOIT ASSUMER CHAQUE ABONNÉ DÉPENDENT DANS UNE LARGE MESURE DES SERVICES AUXQUELS IL S'ABONNE.

LE CÂBLODISTRIBUTEUR DOIT NÉCESSAIREMENT SAVOIR EXACTEMENT QUELS SERVICES L'ABONNÉ REÇOIT AFIN DE DONNER SATISFACTION ET D'ÉTABLIR LA FACTURE PERTINENTE. LA SIMPLE CUEILLETTE DE CES RENSEIGNEMENTS NE DOIT PAS, EN ELLE-MÊME, ÊTRE CONSIDÉRÉE COMME UNE MENACE D'INTRUSION DANS LA VIE PRIVÉE DE L'ABONNÉ. IL NE S'AGIT QUE DE RECUEILLIR LES RENSEIGNEMENTS NÉCESSAIRES À LA FACTURATION TOUT COMME LE FONT PAR EXEMPLE LES SOCIÉTÉS DE TÉLÉPHONE AFIN DE POUVOIR IMPUTER LES FRAIS D'INTERURBAINS.

NOUS COMPTONS OFFRIR UN JOUR UN SERVICE BILATÉRAL AUX ABONNÉS. EN ÉCHANGE DU SERVICE, L'ABONNÉ CORRESPONDRA DIRECTEMENT AVEC LE BUREAU DE LA SOCIÉTÉ DE TÉLÉDISTRIBUTION. L'INDUSTRIE DE LA TÉLÉDISTRIBUTION S'EST PENCHÉE SUR LE PROCESSUS DE CUEILLETTE DE CES DONNÉES INDIVIDUELLES ET A EXAMINÉ SES RESPONSABILITÉS À L'ÉGARD DU TRAITEMENT DE CES DONNÉES ET DE LA MESURE DANS LAQUELLE CES RENSEIGNEMENTS EMPIÈTENT SUR LE DROIT DE CHAQUE ABONNÉ À SA VIE PRIVÉE. TRÈS PEU DE RÉSEAUX DE CÂBLODIFFUSION

OFFRENT DÉJÀ UN SERVICE BILATÉRAL ET, À NOTRE AVIS, IL FAUDRA UN CERTAIN TEMPS AVANT QUE CES SERVICES DEVIENNENT GÉNÉRALISÉS. HEUREUSEMENT, CET INTERVALLE NOUS PERMETTRA D'ÉVALUER LA SITUATION ET D'INVENTER UN CODE PRATIQUE SERVANT À LA FOIS LES INTÉRÊTS DU CONSOMMATEUR ET DE L'INDUSTRIE.

L'ÉTUDE

AU DÉBUT DE 1983, SOIT IMMÉDIATEMENT APRÈS LA MISE EN PLACE DES PREMIERS SERVICES DISCRÉTIONNAIRES, L'INDUSTRIE DE LA CÂBLO-DISTRIBUTION A EFFECTUÉ, PAR L'ENTREMISE DE SON ASSOCIATION NATIONALE, L'ACTC, UNE ÉTUDE SUR LA NÉCESSITÉ D'UN CODE DE PROTECTION DE LA VIE PRIVÉE POUR L'INDUSTRIE. NOUS AVONS D'ABORD EXAMINÉ LES SOCIÉTÉS ÉQUIVALENTES AUX ÉTATS-UNIS OÙ DES SERVICES DISCRÉTIONNAIRES EXISTENT DEPUIS UN CERTAIN NOMBRE D'ANNÉES. NOUS AVONS ÉTUDIÉ LES CODES ACTUELS D'UN CERTAIN NOMBRE DE GRANDES ENTREPRISES DE CÂBLODISTRIBUTION ET D'ASSOCIATIONS AMÉRICAINES, NOTAMMENT LA COX CABLE D'ATLANTA (GÉORGIE), LA NEW JERSEY CABLE TELEVISION ASSOCIATION, LA NEW ENGLAND CABLE TELEVISION ASSOCIATION, LA VIDEOTEX INDUSTRY ASSOCIATION OF WASHINGTON, D.C. ET LE WARNER AMEX CODE OF PRIVACY DONT IL EST SOUVENT QUESTION. NOUS AVONS ÉGALEMENT EXAMINÉ LE CODE DE PROTECTION DE LA VIE PRIVÉE ÉTABLI À DES FINS INTERNES PAR ROGERS CABLE, LE CÂBLODISTRIBUTEUR LE PLUS IMPORTANT AU CANADA.

CETTE ÉTUDE NOUS A PERMIS D'ÉTABLIR UN CODE DE PROTECTION DE LA VIE PRIVÉE QUI, À NOTRE AVIS, PROTÉGERA CONVENABLEMENT LES INTÉRÊTS DES ABONNÉS DU CÂBLE AU CANADA. NOTRE CONSEIL D'ADMINISTRATION L'A EXAMINÉ AU DÉBUT DE L'ANNÉE ET IL EN A RECOMMANDÉ L'ADOPTION AUX MEMBRES DE L'ASSOCIATION NATIONALE. LE CODE PROPOSÉ FERA L'OBJET DE DISCUSSIONS À L'ASSEMBLÉE GÉNÉRALE ANNUELLE QUI DOIT AVOIR LIEU À OTTAWA AU COURS DE LA DEUXIÈME SEMAINE DE JUIN. NOUS ESPÉRONS QU'À CE MOMENT-LÀ, IL SERA GÉNÉRALEMENT ACCEPTÉ PAR LES MEMBRES DE L'ASSOCIATION.

CODE

JE NE SUIS MANIFESTEMENT PAS AUTORISÉ À RENDRE PUBLIC LE PROJET DE CODE TANT QU'IL N'AURA PAS ÉTÉ ACCEPTÉ PAR LES MEMBRES, MAIS JE PUIS NÉANMOINS RÉSUMER LES PRINCIPALES PRÉOCCUPATIONS AUXQUELLES IL S'ATTAQUE.

LA CUEILLETTE DE RENSEIGNEMENTS :

LE CODE EXIGERA QUE CHAQUE ABONNÉ SOIT MIS AU COURANT DES RENSEIGNEMENTS QUI SONT RECUEILLIS ET DES RAISONS DE CETTE CUEILLETTE DE RENSEIGNEMENTS. SEULS LES RENSEIGNEMENTS INDISPENSABLES À LA FACTURATION OU À LA PRESTATION D'UN SERVICE CONVENABLE À L'ABONNÉ SERONT RECUEILLIS. LES RENSEIGNEMENTS EN QUESTION NE SERONT CONSERVÉS QUE LE TEMPS NÉCESSAIRE À CES DEUX FINS, APRÈS QUOI ILS SERONT DÉTRUITS.

LA SÉCURITÉ :

TOUTES LES MESURES ACCEPTABLES SERONT PRISES AFIN D'ASSURER LA SÉCURITÉ DES RENSEIGNEMENTS RECUEILLIS. SEULS LES EMPLOYÉS PARTICIPANTS DIRECTEMENT À LA PRESTATION DES SERVICES AURONT ACCÈS À CES DONNÉES.

ACCÈS PAR L'ABONNÉ :

DANS DES LIMITES RAISONNABLES, LES ABONNÉS POURRONT EXAMINER LES RENSEIGNEMENTS VERSÉS À LEURS DOSSIERS ET ILS AURONT LE DROIT DE FAIRE CORRIGER LES ERREURS.

LES TIERS :

TOUT TIERS QUI PARTICIPERA À LA PRESTATION DE SERVICES AUX ABONNÉS DE LA SOCIÉTÉ DE CÂBLODISTRIBUTION DEVRA RESPECTER LES POLITIQUES CONCERNANT LA VIE PRIVÉE.

LE RESPECT DE LA LOI :

DES RENSEIGNEMENTS CONCERNANT UN ABONNÉ NE SERONT TRANSMIS AUX ORGANISMES GOUVERNEMENTAUX QUE SI UNE ORDONNANCE D'UN TRIBUNAL OU UN AUTRE INSTRUMENT JURIDIQUE L'EXIGE. PAR AILLEURS, À MOINS D'INTERDICTION PAR LA LOI, LES ABONNÉS SERONT MIS AU COURANT DE CES DEMANDES LÉGALES DES RENSEIGNEMENTS.

LA RÉVISION DES POLITIQUES :

FINALEMENT, ÉTANT DONNÉ QUE NOTRE INDUSTRIE ÉVOLUE TRÈS RAPIDEMENT, IL FAUT ÉTABLIR UNE DISPOSITION DE RÉVISION DU CODE DE PROTECTION DE LA VIE PRIVÉE POUR FAIRE EN SORTE QU'IL TIENNE CONVENABLEMENT COMPTE DE L'ÉVOLUTION SUR LES PLANS JURIDIQUE ET TECHNOLOGIQUE.

ITION DE
NDUSTRIE

NOUS CROYONS QU'UN CODE VOLONTAIRE RÉPONDRA CONVENABLEMENT AUX BESOINS DE L'INDUSTRIE DE LA CÂBLODISTRIBUTION EN MATIÈRE DE PROTECTION DE LA VIE PRIVÉE ET QU'IL OFFRIRA LA SOUPLESSE INDISPENSABLE POUR PERMETTRE À CETTE INDUSTRIE DE S'ADAPTER AUX CHANGEMENTS RAPIDES QUI CARACTÉRISENT LES CONDITIONS DANS LESQUELLES L'INDUSTRIE ÉVOLUE. BON NOMBRE CONSIDÈRENT LA CÂBLODISTRIBUTION COMME UN MONOPOLE OR, MÊME SI SE FUT LE CAS À UN MOMENT DONNÉ, CE NE L'EST PLUS AUJOURD'HUI. DE NOS JOURS, LES SOCIÉTÉS DE CÂBLODISTRIBUTION DOIVENT SOUTENIR LA CONCURRENCE DE DIVERS AUTRES SERVICES QUI RIVALISENT AVEC ELLES POUR OBTENIR L'ATTENTION ET L'ARGENT DES ABONNÉS. IL S'AGIT NOTAMMENT DU THÉÂTRE EN DIRECT, DES ANTENNES DOMESTIQUES PLUS COMPLEXES, DES STATIONS TERRESTRES QUI CAPTENT UNE GRANDE VARIÉTÉ D'ONDES TRANSMISES PAR SATELLITES ET, ÉVIDEMMENT, DES MAGNÉTOSCOPES DOMESTIQUES POUR LESQUELS LE MARCHÉ A RÉCEMMENT AUGMENTÉ

LA RÉGLEMENTATION GOUVERNEMENTALE N'EST PAS NOUVELLE POUR NOTRE INDUSTRIE. LE CONSEIL DE LA RADIODIFFUSION ET DES TÉLÉCOMMUNICATIONS CANADIENNES RÉGLEMENTE FORTEMENT LES ACTIVITÉS DES RÉSEAUX DE CÂBLODISTRIBUTION. TOUTEFOIS, MÊME CE CONSEIL A RECONNU LA NÉCESSITÉ D'ALLÉGER, DANS LA MESURE DU POSSIBLE, LE FARDEAU DE LA RÉGLEMENTATION AFIN DE PERMETTRE À L'INDUSTRIE DE LA CÂBLODISTRIBUTION DE SOUTENIR ADÉQUATEMENT LA CONCURRENCE CROISSANTE À LAQUELLE ELLE FAIT FACE. À NOTRE AVIS, IL SERAIT PRÉMATURÉ QUE LES GOUVERNEMENTS, FÉDÉRAL OU PROVINCIAUX, ADOPTENT DES RÈGLEMENTS DANS CE DOMAINE ALORS QUE LE SECTEUR PRIVÉ PEUT FORT BIEN RÉGLER LE PROBLÈME DE FAÇON SATISFAISANTE.

IL Y A ÉVIDEMMENT UNE AUTRE SOLUTION. UN ÉCRIVAIN BIEN CONNU A DÉJÀ DÉCLARÉ QUE POUR ÉVITER LES INTRUSIONS DANS NOTRE VIE PRIVÉE, IL FALLAIT TOUT SIMPLEMENT RENDRE NOS AFFAIRES TELLEMENT ENNUYANTES QUE PERSONNE NE VOUDRA RIEN SAVOIR DE NOUS DE TOUTE FAÇON.

JE VOUS REMERCIE.

CA1

Z4

C52

INTERPROVINCIAL CONFERENCE ON PRIVACY:
INITIATIVES FOR 1984 (SYMPOSIUM)

Remarks to a Panel Discussion on
"Transborder Data Flow: The Trends, The Issues"

James C. Grant
Vice-President
Strategic Planning, Retail Banking
The Royal Bank of Canada



Toronto, Ontario
May 23-24, 1984



Royal Bank News



For Release

10:00 a.m. E.D.T.
Thursday, May 24, 1984

NOTE TO EDITORS/NEWS DIRECTORS

In the attached speech delivered today in Toronto to a Conference on Privacy, sponsored by the Ontario Government, J.C. Grant, Vice-President, Strategic Planning, Retail Banking, The Royal Bank of Canada, addresses the issues of transborder information flows and protection of privacy. He points out the importance of uniformity of regulation and international harmonization in the area of privacy protection and calls for Canadian government and business to co-operate in establishing uniform guidelines in this area.

HIGHLIGHTS

- Protection of privacy is important and must be built into information processing systems. (Pg. 3)
- Privacy laws, regulations and codes should be consistent enough to offer individuals the same basic protection of personal information regardless of where the information is stored or processed. (Pg. 4)
- Canadian business has a "window of opportunity" to take the initiative in developing privacy standards. (Pg. 5)
- Rules governing privacy must be clear and predictable; sudden changes in government policy can jeopardize large investments in computer technology. (Pg. 7)
- Canada's privacy protection rules should be in harmony with those of its main trading partners, especially the U.S. (Pg. 8)
- Ready access to information services, both internationally and inter-provincially, is essential to Canada's economic growth. (Pg. 10)
- There is a danger that countries will act unilaterally to restrict the kind of information that can be sent, processed or stored abroad; the threat of information protectionism is greater for Canada than for larger nations. (Pg. 12)

- 2 -

- . The Royal Bank has proposed the idea of a Canada/U.S. agreement in the area of traded computer services and harmonization of privacy protection. (Pg. 12)
- . Business commitment to rigorous uniform privacy protection codes can help reduce the need for government regulation. (Pg. 19)
- . To negotiate a bilateral Canada/U.S. agreement, the Canadian federal government and provinces must adopt a uniform approach. (Pg. 21)

- 30 -

For further information, please contact:

Jane Lesslie, Toronto, (416) 865-6159

Walter Tedman, Toronto, (416) 865-4796

JAMES C. GRANT
VICE-PRESIDENT
STRATEGIC PLANNING, RETAIL BANKING
THE ROYAL BANK OF CANADA

REMARKS TO A PANEL DISCUSSION ON

"TRANSBORDER DATA FLOW: THE TRENDS, THE ISSUES"

CONFERENCE ON PRIVACY: INITIATIVES FOR 1984
TORONTO, ONTARIO
MAY 24, 1984

SPONSORED BY
THE HONOURABLE NORMAN STERLING, Q.C.
PROVINCIAL SECRETARY FOR RESOURCES DEVELOPMENT,
ONTARIO

MEDIA VERSION OF J.C. GRANT'S SPEECH TO:
"CONFERENCE ON PRIVACY: INITIATIVES FOR 1984"
TORONTO - MAY 24, 1984

I WOULD LIKE TO JOIN MY FELLOW PANELISTS AND CONFERENCE
SPEAKERS IN WELCOMING THE GOVERNMENT OF ONTARIO'S INITIATIVE IN
BRINGING TOGETHER REPRESENTATIVES FROM OTTAWA, THE PROVINCES AND
TERRITORIES AND THE PRIVATE SECTOR TO DISCUSS PRIVACY AND RELATED
ISSUES. I AM PLEASED TO NOTE THAT THE VIEWS OF THE PRIVATE SECTOR
HAVE BEEN ACTIVELY SOUGHT. ON BEHALF OF MY BUSINESS COLLEAGUES,
AND CERTAINLY ON BEHALF OF THE ROYAL BANK, I AM HAPPY TO
CONTRIBUTE TO THE DISCUSSION OF THESE ISSUES.

LET ME BEGIN BY TRYING TO PIN DOWN WHAT IS MEANT BY THE PHRASE "TRANSBORDER DATA FLOWS". IT WAS COINED, IF I AM NOT MISTAKEN, BY TODAY'S CHAIRMAN, RUSS PIPE, AT THE O.E.C.D.'S FIRST CONFERENCE ON THE ISSUE IN 1977. IT IS A BIT OF A CATCH-ALL THAT COVERS A COMPLEX OF INTERRELATED SUBJECTS -- FROM ACCESS TO COMPUTER SERVICES AND TELECOMMUNICATIONS STANDARDS TO COPYRIGHT LAW, BROADCASTING, CULTURAL POLICY AND PRIVACY. I SOMETIMES WONDER IF THERE ARE ANY ACTIVITIES THAT DO NOT SOMEHOW RELATE TO THE TRANSMISSION OF INFORMATION ACROSS NATIONAL BOUNDARIES.

THIS MORNING, I WOULD LIKE TO DISCUSS TWO SUBJECTS THAT FALL UNDER THE UMBRELLA OF TRANSBORDER DATA FLOWS. ONE, PRIMARILY ECONOMIC, IS THE EXCHANGE OF COMMERCIAL INFORMATION, TECHNOLOGY, KNOWLEDGE AND COMPUTER SERVICES. THE OTHER, PRIMARILY A HUMAN RIGHTS CONCERN, IS PRIVACY PROTECTION.

IT HAS BEEN SUGGESTED THAT ECONOMIC EFFICIENCY DEPENDS ON THE "FREE FLOW" OF INFORMATION ACROSS NATIONAL BORDERS. IN FACT, I DOUBT THAT TOTALLY FREE INFORMATION FLOWS EXIST OR EVEN THAT THEY ARE DESIRABLE. ELECTRONIC HIGHWAYS NEED RULES OF THE ROAD. JUST AS TECHNICAL RULES ARE NEEDED BY COMPUTER AND TELECOMMUNICATIONS ENGINEERS, RULES ON ACCESS TO SERVICE AND MARKETS ARE NEEDED TO CREATE A PREDICTABLE ENVIRONMENT FOR BUSINESS PLANNERS. IT IS ALSO EVIDENT THAT RULES ARE NEEDED TO PROTECT SENSITIVE NATIONAL INTERESTS, BE THEY ECONOMIC, CULTURAL OR LEGAL.

THERE ARE FEW NATIONAL INTERESTS MORE SENSITIVE THAN THAT OF PRIVACY PROTECTION. PRIVACY IS IMPORTANT FOR TWO MAIN REASONS.

FIRST, IN THE "INFORMATION AGE", PRIVACY PROTECTION IS IMPORTANT IN ITS OWN RIGHT. PEOPLE DEMAND IT, ALTHOUGH IT IS NOT ENTIRELY CLEAR WHAT EXACTLY THEY WANT. ABUSES ARE POSSIBLE AND PROTECTION MUST BE "BUILT IN" TO INFORMATION PROCESSING SYSTEMS.

SECOND, GIVEN THE VOLUME AND ECONOMIC IMPORTANCE OF TRANSBORDER INFORMATION FLOWS, UNIFORMITY IN THE FUNDAMENTAL GROUND RULES OF PRIVACY PROTECTION IS IMPORTANT. PRIVACY LAWS, REGULATIONS AND CORPORATE CODES NEED NOT ALWAYS BE IDENTICAL. BUT THEY DO NEED TO BE CONSISTENT ENOUGH TO OFFER INDIVIDUALS THE SAME BASIC PROTECTION OF PERSONAL INFORMATION, NO MATTER WHERE IT IS STORED OR PROCESSED.

GOVERNMENTS ARE NOT ALONE IN APPRECIATING THE IMPORTANCE OF PRIVACY PROTECTION. BANKS, FOR EXAMPLE, DEPEND AS MUCH ON PUBLIC CONFIDENCE AS GOVERNMENTS DO ON VOTER CONFIDENCE. OUR CUSTOMERS ALSO HAPPEN TO BE GOVERNMENTS' EMPLOYERS. WHETHER THEY WEAR CONSUMERS' OR VOTERS' HATS, THEY ARE CONCERNED WITH WHAT HAPPENS TO THE PERSONAL INFORMATION STORED IN THE AUTOMATED DATA BASES OF BOTH BUSINESS AND GOVERNMENT.

AS WE HEARD IN EARLIER CONFERENCE SESSIONS, NORTH AMERICAN PRIVACY LEGISLATION APPLIES MAINLY TO THE PUBLIC SECTOR AND IS, IN ANY CASE, STILL IN ITS FORMATIVE STAGES. THIS GIVES CANADIAN BUSINESS WHAT I THINK IS A "WINDOW OF OPPORTUNITY" TO TAKE THE INITIATIVE IN DEVELOPING PRIVACY STANDARDS. THESE STANDARDS SHOULD BE RIGOROUS ENOUGH TO PROVIDE FULL PUBLIC CONFIDENCE WITHOUT INTRODUCING ECONOMIC INEFFICIENCIES -- A FLEXIBLE APPROACH, IN OTHER WORDS.

BUT FLEXIBILITY DOES NOT MEAN CREATING LOOPHOLES AND FIDDLING THE RULES. IT MEANS ADAPTING FUNDAMENTAL STANDARDS OF PRIVACY PROTECTION TO SPECIFIC INDUSTRIES AND ORGANIZATIONS. FOR EXAMPLE, MANY BANK CUSTOMERS EXPECT BANKS TO RETAIN CREDIT FILES EVEN AFTER A LOAN IS RETIRED. PART OF THEIR REASON FOR DEALING WITH US IS TO BUILD A WIDELY ACCEPTED CREDIT RATING WHICH THEY WANT DISCLOSED IN

APPROPRIATE CIRCUMSTANCES AND WITH PRUDENT SAFEGUARDS. FLEXIBLE STANDARDS ARE NOT JUST MORE ECONOMICALLY EFFICIENT, THEY CAN ALSO BE MORE EFFECTIVE IN PROTECTING PRIVACY.

BUSINESS REALIZES THAT IF IT FAILS TO REGULATE ITSELF TO THE PUBLIC'S SATISFACTION, IT IS LEAVING THE DOOR OPEN TO DETAILED GOVERNMENT REGULATION. AND I, FOR ONE, WOULD BE VERY PLEASED TO RELIEVE CIVIL SERVANTS OF THAT BURDEN. WITHIN MY INDUSTRY, THE CANADIAN BANKERS' ASSOCIATION AND ITS MEMBER BANKS, INCLUDING THE ROYAL, ARE CURRENTLY STUDYING THE ISSUE OF PRIVACY PROTECTION WITH CONSIDERABLE CARE.

IN WORKING WITH GOVERNMENT AND THE PUBLIC TO BUILD A CONSENSUS ON PRIVACY, BUSINESS WILL HAVE SEVERAL PRIME CONCERNS IN MIND.

ONE IS THAT THE "RULES OF THE ROAD" BE CLEAR AND PREDICTABLE. THIS IS ESSENTIAL IF MODERN BUSINESS IS TO MAKE OPTIMUM USE OF COMPUTER TECHNOLOGY TO PROMOTE EFFICIENCY AND COMPETITIVENESS, PARTICULARLY IN INTERNATIONAL MARKETS. SUDDEN CHANGES IN GOVERNMENT POLICY CAN JEOPARDIZE LARGE INVESTMENTS IN EQUIPMENT, RESEARCH AND DEVELOPMENT AND SYSTEMS ENGINEERING.

ANOTHER CONCERN IS THAT THE RULES BE UNIFORM WITHIN CANADA.

ONE WOULD THINK THAT, AS A MATTER OF PUBLIC POLICY, CANADIANS SHOULD HAVE THE SAME BASIC PRIVACY RIGHTS FROM COAST TO COAST. THERE IS ALSO A PRESSING ECONOMIC REASON FOR UNIFORMITY IN A FEDERAL STATE WITH A SMALL DOMESTIC MARKET. DISRUPTIONS IN INTER-PROVINCIAL INFORMATION FLOWS COULD DEPRIVE CANADA OF ITS COMMON MARKET IN COMPUTER SERVICES. IDENTIFYING UNIFORM PRIVACY RIGHTS SHOULD BE STRAIGHTFORWARD. MORE DIFFICULT, BUT NEVERTHELESS VITAL, IS THE UNIFORMITY OF REGULATORY MECHANISMS.

THIS WILL REQUIRE THE PRECISE MESHING OF FEDERAL, PROVINCIAL AND PRIVATE SECTOR CODES.

A THIRD CONCERN OF BUSINESS IS THAT CANADA'S PRIVACY PROTECTION RULES BE IN HARMONY WITH THOSE OF OUR MAIN TRADING PARTNERS, IN PARTICULAR THE UNITED STATES. OTHERWISE, CANADIAN FIRMS COULD FACE INCREASED RISK AND COST IN A HIGHLY COMPETITIVE ENVIRONMENT.

THE SEARCH FOR WIDELY ACCEPTED PRINCIPLES OF PRIVACY PROTECTION SHOULD BEGIN WITH THE O.E.C.D. GUIDELINES ON PRIVACY AND TRANSBORDER FLOWS OF PERSONAL INFORMATION. THEY PROVIDE VALUABLE REFERENCE POINTS FOR BOTH INTERNATIONAL AND FEDERAL/PROVINCIAL HARMONIZATION. THE GUIDELINES ARE GAINING ACCEPTANCE. THEY ARE BOTH COMPREHENSIVE AND FLEXIBLE ENOUGH TO REFLECT THE CORE OF PRIVACY RIGHTS COMMON TO CODES, BILLS AND LAWS

IN A NUMBER OF COUNTRIES, INCLUDING CANADA. THE ROYAL BANK, AMONG OTHERS, HAS URGED THE FEDERAL GOVERNMENT TO ENDORSE THEM FORMALLY. THE U.S. GOVERNMENT AND MANY CORPORATIONS OUTSIDE CANADA HAVE ALREADY DONE SO.

I WOULD LIKE TO SPEND THE NEXT FEW MINUTES ON THE RATIONALE FOR MY THREE PRIME CONCERNS -- THE NEED FOR CLEAR PRIVACY RULES, THE NEED FOR UNIFORMITY WITHIN CANADA AND THE NEED FOR HARMONIZATION INTERNATIONALLY. MANAGING THESE ISSUES EFFECTIVELY WILL GREATLY STRENGTHEN CANADA'S INTERNATIONAL COMPETITIVENESS. TO GRASP WHY, IT IS NECESSARY TO UNDERSTAND THE GROWING ECONOMIC IMPORTANCE OF COMPUTERIZED INFORMATION SERVICES.

READY ACCESS TO THESE SERVICES, INTERNATIONALLY AND INTER-PROVINCIALY, IS ESSENTIAL TO EFFICIENCY, WEALTH CREATION AND OUTPUT GROWTH IN ALL SECTORS OF THE CANADIAN ECONOMY. MORE AND MORE INDUSTRIES ARE BECOMING MAJOR USERS OF "HIGH TECH" AS COMPUTER APPLICATIONS PROLIFERATE AND THE COST OF DATA PROCESSING FALLS.

IN THE SERVICE SECTOR, FOR EXAMPLE, WHICH ACCOUNTS FOR 2/3 OF CANADA'S GNP AND AN EVER INCREASING PORTION OF WORLD TRADE, COMPUTERIZED INFORMATION SYSTEMS ARE BOOSTING PRODUCTIVITY AND TRANSFORMING PRODUCT LINES AND DELIVERY SYSTEMS. IN MANUFACTURING, COMPUTERS ARE USED FOR EVERYTHING FROM PRODUCTION TO MARKET RESEARCH, DISTRIBUTION, INVENTORY CONTROL, PRODUCT DESIGN AND FINANCIAL PLANNING.

IN AGRICULTURE, LET ME GIVE YOU AN EXAMPLE FROM THE ROYAL BANK ITSELF. OUR AGROLOGISTS NOW USE PORTABLE COMPUTERS TO HELP FARMERS FORECAST CASH FLOW USING ESTIMATED CROP YIELDS, INPUT COSTS AND WORLD MARKET PRICES. PROJECTIONS THAT USED TO TAKE HOURS ARE DONE IN SECONDS, USING UP-TO-DATE COMPUTERIZED DATA ON COMMODITY PRICES, WEATHER PATTERNS AND SO ON.

TECHNOLOGICAL ADVANCE MAY BE CREATING MANY NEW COST-EFFICIENT INFORMATION SERVICES AND DATA BASES. BUT THEIR UTILITY RESTS ON ENSURED, UNINTERRUPTED ACCESS FOR USERS. CONSIDER THE CASE OF DRESSER INDUSTRIES. YOU MAY RECALL THAT AFTER MARTIAL LAW WAS IMPOSED IN POLAND, THE U.S. GOVERNMENT PROHIBITED THAT FIRM'S FRENCH SUBSIDIARY FROM SUPPLYING EQUIPMENT OR TECHNOLOGY FOR THE TRANS-SIBERIAN GAS PIPELINE. WHAT, MIGHT WE GUESS, HAPPENED TO THE ECONOMIC VALUE AND REPUTATION OF DRESSER FRANCE THE INSTANT IT WAS DENIED ACCESS TO EXPERTISE AND INFORMATION?

IN THE ABSENCE OF INTERNATIONAL AGREEMENTS ENSURING UNINTERRUPTED ACCESS TO INFORMATION SERVICES, BUSINESS FACES AN UNCERTAIN ENVIRONMENT. THERE IS A DANGER THAT COUNTRIES WILL ACT UNILATERALLY TO RESTRICT THE KIND OF INFORMATION THAT CAN BE SENT, PROCESSED OR STORED ABROAD. THE RESULT COULD BE AN ARRAY OF RESTRICTIVE RULES AND REGULATIONS, RANGING FROM TARIFF AND NON-TARIFF BARRIERS TO GOVERNMENT ATTEMPTS TO REGISTER, TAX AND MONITOR ALL DATA BANKS. THE THREAT OF INFORMATION PROTECTIONISM IS GREATER FOR CANADA, WITH ITS RELATIVELY SMALL DOMESTIC MARKET, THAN IT IS FOR LARGER NATIONS AND TRADING BLOCS.

FOR ALL THESE REASONS, THE ROYAL BANK HAS PROPOSED AND ACTIVELY PROMOTED THE IDEA OF A SECTORAL AGREEMENT BETWEEN CANADA AND THE U.S. COVERING WHAT WE CALL "TRADED COMPUTER SERVICES", A BILATERAL AGREEMENT THAT COULD SET THE PATTERN FOR SUBSEQUENT MULTILATERAL LIBERALIZATION. OUR PROPOSAL IS DOUBLE-BARRELLED. ONE BARREL IS AIMED AT ESTABLISHING MUTUALLY ACCEPTABLE TRADING

RULES GOVERNING ACCESS TO MARKETS FOR CANADIAN AND AMERICAN SUPPLIERS, AND ACCESS TO COMPUTER SERVICES FOR CANADIAN AND AMERICAN USERS. THE OTHER BARREL IS AIMED AT THE HARMONIZATION OF PRIVACY PROTECTION IN THE TWO COUNTRIES. I HAVE JUST DISCUSSED THE ECONOMIC AND TRADE ISSUES. LET ME NOW TURN TO PRIVACY.

AN INTERNATIONAL PATCHWORK OF PRIVACY PROTECTION REGIMES COULD HAVE MUCH THE SAME ECONOMIC EFFECT AS OVERT RESTRICTIONS ON INFORMATION TRADE AND EXCHANGES. BUSINESS WOULD BE CONFRONTED WITH THE COSTS AND INEFFICIENCIES OF MULTIPLE REGULATORY COMPLIANCE FROM COUNTRY TO COUNTRY. EVEN WORSE, THERE IS THE RISK THAT GOVERNMENTS WILL INSIST THAT ALL PERSONAL INFORMATION BE PROCESSED IN DOMESTIC DATA BANKS ON THE GROUNDS THAT OTHER COUNTRIES DO NOT OFFER EQUIVALENT PRIVACY PROTECTION. EXCEPT IN EUROPE, INTERNATIONAL GROUND RULES ON PRIVACY ARE HAZY. INFORMATION FLOWS CAN BE DISRUPTED IN ARBITRARY, UNPREDICTABLE WAYS.

ANOTHER SOURCE OF UNCERTAINTY HAS BEEN THE PERCEIVED RISK THAT SOME EUROPEAN COUNTRIES COULD USE PRIVACY PROTECTION AS A SMOKESCREEN FOR TRADE PROTECTIONISM. GOVERNMENT REGULATORS MUST KEEP PRIVACY RIGHTS SEPARATE FROM TRADE ISSUES. PRIVACY PROTECTION IS COMPLEX AND DEMANDING ENOUGH THAT IT WOULD BE UNWISE TO MIX ECONOMIC PROBLEMS IN AS WELL.

THE NOTION OF PRIVACY HAS BECOME QUITE SWEEPING. FROM A BANKER'S PERSPECTIVE, THE EVOLUTION IS INTERESTING. TRADITIONALLY, BANKERS HAVE HAD TO MEET HIGH PUBLIC EXPECTATIONS CONCERNING TWO ASPECTS OF PRIVACY:

THE FIRST IS "SECURITY": BANK VAULTS ARE NOW BEING SUPPLEMENTED BY THE COMPUTERIZED "GATE-KEEPERS" PROTECTING DATA BASES FROM UNAUTHORIZED ACCESS.

THE SECOND ASPECT IS "CONFIDENTIALITY": BANKERS, LIKE DOCTORS AND LAWYERS, ARE CUSTODIANS OF THEIR CLIENTS' INFORMATION. THEY HAVE A CONTRACTUAL DUTY TO DISCLOSE IT TO THIRD PARTIES ONLY IN VERY NARROWLY DEFINED CIRCUMSTANCES, PRINCIPALLY WITH CUSTOMER CONSENT AND UNDER LEGAL COMPLUSION.

BUT "PRIVACY" NOW GOES BEYOND "SECURITY" AND "CONFIDENTIALITY". IT IS VIEWED AS A COMPREHENSIVE SET OF RIGHTS THAT GIVE INDIVIDUALS A DEGREE OF CONTROL OVER PERSONAL INFORMATION -- NOT ONLY OVER HOW IT IS DISCLOSED, BUT ALSO HOW IT IS COLLECTED, PROCESSED, USED, VERIFIED AND CORRECTED IN THE EVENT OF ERROR.

BANKS ARE "INFORMATION INTENSIVE" BUSINESSES, WHICH NEED ACCESS TO PRIVATE PERSONAL INFORMATION TO DO BUSINESS AND WHICH NEED TO MAINTAIN PUBLIC CONFIDENCE TO STAY IN BUSINESS. WE ARE FULLY AWARE THAT OUR POLICIES AND INFORMATION PRACTICES MUST REFLECT THE MODERN CONCEPT OF "PRIVACY". OUR EXPERIENCE WITH "SECURITY" AND "CONFIDENTIALITY" IS A SOLID FOUNDATION TO BUILD ON.

IT IS ESSENTIAL NOT ONLY THAT PRIVACY BE PROTECTED AND PUBLIC TRUST MAINTAINED, BUT, FOR THE ECONOMIC REASONS I HAVE DISCUSSED, THAT VARIOUS NATIONS' PRIVACY REQUIREMENTS BE REASONABLY UNIFORM.

CLEARLY, THE NUMEROUS PRIVACY LAWS PASSED IN EUROPE AND NORTH AMERICA ARE NOT PERFECTLY UNIFORM. THE KEY DIFFERENCES CONCERN ENFORCEMENT METHODS AND THE SCOPE OF REGULATION -- WHETHER IT APPLIES, FOR EXAMPLE, TO THE PUBLIC SECTOR ALONE OR TO THE PRIVATE

SECTOR AS WELL, TO AUTOMATED INFORMATION SYSTEMS OR ALSO TO MANUAL FILES.

MORE IMPORTANT THAN THESE DIFFERENCES, HOWEVER, IS THE FACT THAT THE LEGISLATION TO DATE REFLECTS THE SAME BASIC POLICY CONCERN -- TO GIVE THE INDIVIDUAL A REASONABLE DEGREE OF CONTROL OVER PERSONAL INFORMATION AND IMPOSE CORRESPONDING RULES ON GOVERNMENTS AND CORPORATIONS.

OUTSIDE OF CANADA, IT MAY NOT BE REALISTIC TO IMPLEMENT A SCHEME FOR MAKING ALL PRIVACY LAWS PERFECTLY UNIFORM. BUT IT IS QUITE REALISTIC TO IDENTIFY WHAT THEY HAVE IN COMMON. HEREIN, AS I SUGGESTED EARLIER, LIES THE VALUE OF THE O.E.C.D. GUIDELINES. THEY SET OUT CORE PRINCIPLES OF PRIVACY PROTECTION THAT SHOULD BE SEEN AS THE COMMON MEASURE OF MANY COUNTRIES' PRIVACY CODES, WHETHER THEY ARE IMPOSED BY LEGISLATION, REGULATORY POLICY OR VOLUNTARY COMPLIANCE.

IN THESE CIRCUMSTANCES, THE PRACTICAL QUESTIONS TO ASK ARE:
CAN COUNTRIES "HARMONIZE" THEIR PRIVACY POLICIES WITHOUT HAVING
IDENTICAL REGULATORY FRAMEWORKS? CAN INDIVIDUALS BE ASSURED THAT
THEIR PERSONAL INFORMATION WILL ENJOY THE SAME BASIC PROTECTION
ABROAD THAT IT ENJOYS IN THE HOME COUNTRY? MY ANSWER TO BOTH IS A
QUALIFIED "YES".

ONE QUALIFICATION IS THE ATTITUDE OF GOVERNMENTS. AS I HAVE
SUGGESTED, THEY MUST MAINTAIN A DISCIPLINED SEPARATION OF PRIVACY
FROM TRADE ISSUES. THIS IS AN ESSENTIAL CONDITION FOR
HARMONIZATION.

ANOTHER QUALIFICATION IS THE ATTITUDE OF THE PRIVATE SECTOR. BUSINESS MUST UNDERSTAND THAT RIGOROUS AND UNIFORM CODES FOR PROTECTING PRIVACY CAN GO A LONG WAY TOWARDS REDUCING THE NEED FOR GOVERNMENT REGULATION. IT WILL ALSO REASSURE CITIZENS THAT MULTINATIONAL DATA FLOWS ARE NOT THREATENING.

OF COURSE, NO GOVERNMENT WILL ABANDON ITS CONCERN AND LEAVE THE PRIVATE SECTOR TO DECIDE HOW AND UNDER WHAT CONDITIONS PERSONAL INFORMATION WILL FLOW ACROSS BORDERS. BUT POLITICAL PRESSURE FOR "ME FIRST" PRIVACY LAWS WILL BE RELIEVED ... IF CORPORATIONS ACT TO PUT MEAT ON THE SKELETON OF THE O.E.C.D. GUIDELINES ... IF MULTINATIONALS BEGIN TO ADOPT UNIFORM INDUSTRY-WIDE OR INTER-CORPORATE CODES ... IF COMPANIES SHOW THE PUBLIC THAT THEY ARE TAKING SPECIFIC MEASURES TO REDUCE THE RISK THAT PERSONAL DATA WILL BE MISHANDLED IN FOREIGN DATA BASES AND PROCESSING CENTRES. SUCH PRIVATE SECTOR ACTIONS ARE THE RAW

MATERIAL FOR MORE FORMALIZED HARMONIZATION OF LAWS BY GOVERNMENTS
AS TIME GOES ON.

THE MULTINATIONAL PRIVATE SECTOR SHOULD NOT UNDERESTIMATE ITS
INFLUENCE. IT HAS LONG EXPERIENCE IN OPERATING IN DIFFERENT
POLITICAL, LEGAL AND REGULATORY ENVIRONMENTS. IT ALSO HAS THE
KNOWLEDGE OF INFORMATION TECHNOLOGY WHICH GOVERNMENTS NEED TO
FORMULATE SOUND POLICY.

GOVERNMENT ACTION TO HARMONIZE PRIVACY PROTECTION IS MOST
PRACTICAL WHEN IT IS TAKEN BY NEIGHBOURING COUNTRIES, WITH SIMILAR
LEGAL SYSTEMS. WE ARE ALREADY SEEING THIS IN EUROPE. IT SEEMS TO
ME THAT CANADA AND THE U.S. COULD FOLLOW SUIT AND NEGOTIATE A
NORTH AMERICAN "MODEL AGREEMENT" COVERING SUCH MATTERS AS
INFORMATION RETRIEVAL RIGHTS, EQUIVALENT PROTECTION, MUTUAL
ENFORCEMENT OF COURT ORDERS AND AGREED PROCEDURES FOR DETERMINING

COURT JURISDICTIONS WHEN CITIZENS OF THE TWO COUNTRIES ARE INVOLVED.

BUT CANADA CANNOT NEGOTIATE INTERNATIONAL AGREEMENTS UNLESS THE FEDERAL GOVERNMENT AND PROVINCES ADOPT A UNIFORM APPROACH TO PRIVACY PROTECTION. WE SIMPLY CANNOT ARRIVE AT THE NEGOTIATING TABLE WITH OUR GOVERNMENTS PULLING IN ANYWHERE FROM TWO TO ELEVEN DIFFERENT DIRECTIONS ON SUCH A FUNDAMENTAL HUMAN RIGHTS ISSUE.

THERE IS ALSO, AS I MENTIONED BEFORE, A PURELY DOMESTIC IMPERATIVE FOR UNIFORMITY. CANADA SHOULD PRESERVE ITS COMMON MARKET IN THE FIELD OF INFORMATION FLOWS AND SERVICES. GOVERNMENTS SHOULD CONSIDER THE BUSINESS COST IMPLICATIONS OF DIFFERING REGULATORY REGIMES. EVEN TODAY, MINOR DIFFERENCES IN SUCH AREAS AS INTEREST RATE CALCULATIONS AND FINANCIAL REPORTING

REQUIREMENTS CAN FORCE CORPORATIONS TO DEVELOP ENTIRELY DIFFERENT COMPUTER PROGRAMS AND SOFTWARE APPLICATIONS FOR DIFFERENT JURISDICTIONS. THE SAME PROBLEM COULD ARISE IF PRIVACY PROTECTION REQUIREMENTS DIVERGE FROM ONE GOVERNMENT TO THE NEXT.

AS A BUSINESSMAN, I DO NOT HAVE STRONG FEELINGS ABOUT THE PRECISE DEFINITION OF FEDERAL/PROVINCIAL JURISDICTIONAL BOUNDARIES IN THE FIELD OF PRIVACY. WHAT IS TERRIBLY IMPORTANT IS THAT ALL CANADA'S GOVERNMENTS START BY "AGREEING TO AGREE" ON A UNIFORM, NATIONWIDE SET OF PRIVACY RIGHTS FOR ALL CANADIANS. MY EXPERIENCE IS THAT CANADIANS EXPECT TO HAVE IDENTICAL PRIVACY RIGHTS, NO MATTER WHERE THEY LIVE OR WHERE IN FUTURE THEY MIGHT MOVE WITHIN CANADA. IF MY PERCEPTION IS RIGHT, GOVERNMENTS WOULD HAVE TO BE POLITICALLY MOTIVATED TO TAKE A SHARED APPROACH.

IF AGREEMENT ON PRIVACY RIGHTS CAN BE REACHED, WE CAN THEN
TURN TO THE QUESTION OF THE RESPECTIVE ROLES OF OTTAWA, THE
PROVINCES AND TERRITORIES AND THE PRIVATE SECTOR IN ENSURING THAT
PRIVACY RIGHTS ARE RESPECTED.

IN ATTEMPTING TO ARRIVE AT A UNIFORM REGULATORY FRAMEWORK,
ALL GOVERNMENTS SHOULD BE AWARE TO THE ROLE WHICH THE PRIVATE
SECTOR CAN PLAY. CORPORATIONS, INDUSTRY ASSOCIATIONS AND OTHER
PRIVATE SECTOR GROUPS CAN ASSIST GOVERNMENT IN ENSURING THAT
FUNDAMENTAL PRIVACY PROTECTION PRINCIPLES ARE IMPLEMENTED
EFFECTIVELY AND EVENLY THROUGHOUT THE COUNTRY. EFFECTIVE SELF
REGULATION, IF IT BECOMES INTEGRAL TO THE ENFORCEMENT OF PRIVACY
RIGHTS, CAN ASSIST THE PROCESS OF FEDERAL/PROVINCIAL CONSENSUS
BUILDING. FOR SELF REGULATION TO BE EFFECTIVE, IT WOULD HAVE TO
REFLECT A NATIONAL CONSENSUS ON PRIVACY.

PRIVACY PROTECTION IS AN IMPORTANT ISSUE, ONE WHICH REQUIRES EXTENSIVE DISCUSSION BY ALL INTERESTED PARTIES. THANKS TO THIS CONFERENCE, IT HAS BEEN DISCUSSED IN SPADES. THANK YOU FOR THIS OPPORTUNITY TO PARTICIPATE.

DOCUMENT: 870-123/016

CAI
Z4
- C52

CONFÉRENCE INTERPROVINCIALE SUR LA PROTECTION
DES RENSEIGNEMENTS PERSONNELS:
MESURES POUR 1984 (COLLOQUE)

Remarques adressées à un groupe de travail sur
"La transmigration des données: tendances et problèmes"

James C. Grant

Vice-président

Planification stratégique, Services bancaires aux particuliers

La Banque Royale du Canada



Toronto, Ontario

23-24 mai 1984

NOTE AUX ÉDITEURS/DIRECTEURS DES NOUVELLES

Dans le discours ci-joint prononcé aujourd'hui à Toronto, lors d'une conférence sur la protection des renseignements personnels parrainée par le Gouvernement de l'Ontario, M. J.C. Grant, vice-président, Planification stratégique, Services bancaires aux particuliers, Banque Royale du Canada, se penche sur les problèmes de la transmigration des renseignements et de la protection des renseignements personnels. Il souligne l'importance de l'uniformité de la réglementation et d'une harmonisation internationale en matière de protection des renseignements personnels; il invite également le gouvernement canadien et le monde des affaires à coopérer pour établir des lignes directrices uniformes en cette matière.

POINTS SAILLANTS

- . La protection des renseignements personnels est une réalité importante, qui doit faire partie intégrante des systèmes de traitement de l'information. (p.)
- . La législation, les règlements et les codes sur la protection des renseignements personnels devraient être suffisamment uniformes pour offrir aux individus la même protection fondamentale à l'égard des renseignements personnels qui les concernent, quel que soit l'endroit où ces renseignements sont emmagasinés ou traités. (p.)

- . Le monde des affaires canadien dispose d'un "créneau" lui permettant de prendre l'initiative dans l'élaboration de normes sur la protection des renseignements personnels. (p.)
- . Les règles régissant la protection des renseignements personnels doivent être claires et prévisibles; les modifications soudaines des orientations du gouvernement peuvent mettre en danger les investissements importants faits en matière de technologie informatique. (p.)
- . Les règles du Canada sur la protection des renseignements personnels devraient s'harmoniser avec celles de ses principaux partenaires commerciaux, et particulièrement les États-Unis. (p.)
- . Un accès facile aux services d'information, tant sur le plan international qu'interprovincial, est essentiel à la croissance économique du Canada. (p.)
- . Il existe un danger que certains pays restreignent unilatéralement les catégories d'informations qui peuvent être envoyées, traitées ou emmagasinées à l'étranger; cette menace du protectionnisme de l'information est plus grande pour le Canada que pour les pays plus importants. (p.)
- . La Banque Royale a avancé l'idée d'une entente Canada/É.-U. dans le domaine des services d'informatique partagés et de l'harmonisation de la protection des renseignements personnels. (p.)

- Les engagements pris par le monde des affaires en vue de codes rigoureux et uniformes de protection des renseignements personnels peuvent contribuer à réduire la nécessité d'une réglementation gouvernementale. (p.)

- Le Gouvernement fédéral canadien et les provinces doivent adopter une approche uniforme pour négocier une entente bilatérale Canada/É.-U. (p.)

Pour de plus amples renseignements, veuillez contacter:

Jane Lesslie, Toronto, (416) 865-6159

Walter Tedman, Toronto, (416) 865-4796

JAMES C. GRANT

VICE-PRÉSIDENT

PLANIFICATION STRATÉGIQUE, SERVICES BANCAIRES AUX PARTICULIERS

LA BANQUE ROYALE DU CANADA

REMARQUES ADRESSÉES À UN GROUPE DE TRAVAIL SUR

"LA TRANSMIGRATION DES DONNÉES: TENDANCES ET PROBLÈMES"

CONFÉRENCE SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS:

MESURES POUR 1984

TORONTO, ONTARIO

24 MAI 1984

PARRAINÉE PAR

L'HONORABLE NORMAN STERLING, C.R.

SECRÉTAIRE PROVINCIAL POUR LE DÉVELOPPEMENT DES RESSOURCES

ONTARIO

Discours prononcé par M. J.C. Grant lors de:

"La conférence sur la protection des renseignements

personnels: mesures pour 1984"

Toronto, 24 mai 1984

Version à l'intention des médias

J'aimerais me joindre à mes collègues du groupe de travail et aux conférenciers pour féliciter le gouvernement de l'Ontario de l'initiative qu'il a prise en réunissant des représentants d'Ottawa, des provinces, des territoires et du secteur privé afin de débattre de la protection des renseignements personnels et des problèmes connexes. Je constate avec plaisir qu'on a activement sollicité le point de vue du secteur privé. Au nom de mes collègues du milieu des affaires, et en celui de la Banque Royale, je suis heureux de contribuer au débat sur ces problèmes.

Permettez-moi de commencer en essayant de préciser ce que signifie l'expression "transmigration des données". Si je ne m'abuse, elle a été forgée par le président d'aujourd'hui, M. Russ Pipe, lors de la première conférence de l'O.C.D.E. sur ce sujet, en 1977. C'est un peu une expression passe-partout, qui englobe un grand nombre de sujets interreliés, allant de l'accès aux services informatiques et des normes de télécommunication à la législation sur les droits d'auteur, en passant par la radiodiffusion, la politique culturelle et la protection des renseignements personnels. Je me demande parfois s'il existe une activité qui ne soit pas reliée d'une façon quelconque à la transmission des renseignements par delà les frontières nationales.

J'aimerais vous entretenir ce matin de deux sujets qui relèvent du domaine de la transmigration des données. L'un d'entre eux, de nature surtout économique, a trait à l'échange de renseignements commerciaux, de technologie, de connaissances et de services informatiques. L'autre, qui concerne principalement les droits de la personne, a trait à la protection des renseignements personnels.

Il a été avancé que l'efficacité économique dépend de la "libre circulation" de l'information par delà les frontières nationales. En fait, je doute que des échanges d'informations entièrement libres existent, voire même qu'ils soient souhaitables. Il nous faut adopter un code de la route pour les autoroutes électroniques. Tout comme les ingénieurs en informatique et en télécommunications ont besoin de règles techniques, il faut avoir des règles sur l'accès aux services et aux marchés afin de créer un environnement stable pour les responsables de la planification commerciale. Il est tout aussi évident qu'il faut adopter des règles pour protéger les intérêts nationaux névralgiques, qu'ils soient économiques, culturels ou juridiques.

Il existe peu d'intérêts nationaux qui soient plus névralgiques que celui de la protection des renseignements personnels. Celle-ci est importante pour deux raisons principales.

Tout d'abord, dans cette "ère de l'information", la protection des renseignements personnels est importante en elle-même. Les gens l'exigent, mais on ne sait pas exactement ce qu'ils désirent. Il existe

des possibilités d'abus et la protection doit faire "partie intégrante" des systèmes de traitement de l'information.

Deuxièmement, étant donné le volume et l'importance économique de la transmigration des renseignements, l'uniformité des règles fondamentales de la protection des renseignements personnels est importante. Il n'est pas toujours nécessaire que les lois, les règlements et les codes privés sur la protection des renseignements personnels soient identiques. Mais ils doivent être suffisamment uniformes pour offrir aux individus la même protection fondamentale à l'égard des renseignements personnels qui les concernent, peu importe l'endroit où ils sont emmagasinés ou traités.

Les gouvernements ne sont pas les seuls à réaliser l'importance de la protection des renseignements personnels. Les banques, par exemple, sont aussi dépendantes de la confiance du public que les gouvernements le sont de la confiance de leurs électeurs. Nos clients sont également les employeurs des gouvernements. Que ce soit en leur qualité de consommateurs ou d'électeurs, ils se préoccupent du sort des renseignements personnels contenus dans les bases de données informatiques des entreprises et du gouvernement.

Comme on nous l'a mentionné lors de séances antérieures de cette conférence, la législation nord-américaine sur la protection des renseignements personnels s'applique surtout au secteur public et n'en est, de toute façon, qu'à ses débuts. À mon avis, cela ouvre au milieu des affaires canadien un "créneau", qui lui permettrait de prendre

l'initiative dans l'élaboration de normes sur la protection des renseignements personnels. Ces normes devraient être suffisamment strictes pour donner entière confiance au public, sans susciter l'inefficacité économique -- autrement dit, une approche flexible.

Toutefois, le fait d'adopter une telle approche ne signifie pas de prévoir des échappatoires et contourner les règles; cela signifie d'adapter les normes fondamentales de protection des renseignements personnels à des industries et à des organisations spécifiques. Par exemple, de nombreux clients des banques s'attendent à ce que les banques conservernt leur dossier de crédit, même après le remboursement d'un prêt. Ils traitent en partie avec nous pour se constituer un dossier de crédit largement accepté, dont ils acceptent la communication dans les circonstances qui la justifient, et avec certaines précautions. Des normes flexibles ne sont pas seulement plus efficaces sur le plan économique; elles peuvent également être plus efficaces pour la protection des renseignements personnels.

Le milieu des affaires est conscient qu'il ouvre la porte à une réglementation gouvernementale détaillée s'il ne s'autoréglemente pas à la satisfaction du public. Je serais personnellement très heureux d'enlever ce fardeau aux fonctionnaires. Dans notre secteur, l'Association des banquiers canadiens et les banques qui en sont membres, y compris la Banque Royale, étudient actuellement le problème de la protection des renseignements personnels avec une très grande attention.

Le milieu des affaires tiendra compte de plusieurs considérations fondamentales en travaillant, de concert avec le gouvernement et le public, à élaborer un consensus sur la protection des renseignements personnels.

L'une d'entre elles est que le "code de la route" doit être clair et prévisible. Cela est essentiel pour que les entreprises modernes puissent faire une utilisation optimale de la technologie de l'informatique, afin de promouvoir l'efficacité et la concurrence, particulièrement sur les marchés internationaux. Des modifications soudaines dans les orientations gouvernementales peuvent mettre en danger les investissements importants consentis en matériel, en recherche et développement et dans la configuration des systèmes.

L'autre préoccupation est que les règles devraient être uniformes au Canada. Il semble légitime de penser que les Canadiens devraient bénéficier en principe des mêmes droits fondamentaux sur la protection des renseignements personnels d'un océan à l'autre. Une raison économique majeure milite également en faveur de l'uniformité dans un état fédéral ayant un marché intérieur restreint: des interruptions dans les échanges interprovinciaux de renseignements pourraient priver le Canada de son marché commun des services d'informatique. On devrait déterminer clairement des droits uniformes à la protection des renseignements personnels. Plus complexe, mais néanmoins vitale, est l'uniformité des mécanismes réglementaires. Cela exigera une coordination étroite des codes des gouvernements fédéral, provinciaux et du secteur privé.

Le milieu des affaires a une troisième préoccupation: les règles sur la protection des renseignements personnels du Canada devraient s'harmoniser avec celles de nos principaux partenaires commerciaux, et en particulier les États-Unis. Sinon, les entreprises canadiennes pourraient s'exposer à une augmentation des risques et des frais dans un environnement extrêmement concurrentiel.

Les lignes directrices de l'O.C.D.E. sur la protection et les échanges internationaux de renseignements personnels devraient constituer le point de départ d'une recherche sur des principes largement acceptés de protection des renseignements personnels. Ces lignes directrices constituent un point de référence valable à la fois pour une harmonisation internationale et fédérale/provinciale. Ces lignes directrices sont de plus en plus reconnues; elles sont à la fois suffisamment complètes et flexibles pour refléter l'essentiel des droits à la protection des renseignements personnels que l'on retrouve dans les codes, les projets de loi et les lois de nombreux pays, y compris le Canada. La Banque Royale, entre autres, a pressé le gouvernement fédéral de les adopter officiellement, ce que le gouvernement des États-Unis et de nombreuses sociétés à l'extérieur du Canada ont déjà fait.

J'aimerais consacrer les prochaines minutes à exposer le fondement de mes trois principales préoccupations: la nécessité de règles claires sur la protection des renseignements personnels; la nécessité d'une uniformité au Canada; et la nécessité d'une harmonisation internationale. La compétitivité internationale du Canada en ressortira grandement

renforcée, si l'on peut solutionner efficacement ces problèmes. Pour en saisir les raisons, il est nécessaire de comprendre l'importance économique croissante des services d'information informatisés.

Un accès facile à ces services, tant au niveau international qu'interprovincial, est essentiel à l'efficacité, à la création de la richesse et à la croissance de la production dans tous les secteurs de l'économie canadienne. Un nombre croissant d'industries deviennent de grands utilisateurs de "haute technologie", tandis que les applications de l'informatique se multiplient et que le coût du traitement des données s'abaisse.

Dans le secteur des services, par exemple, qui représente 2/3 du PNB canadien et une part toujours croissante du commerce mondial, les systèmes d'information informatisés accroissent la productivité et transforment les lignes de produits et les systèmes de livraison. Dans le secteur secondaire, les ordinateurs sont utilisés pour toutes les fonctions, de la production aux recherches de marché, en passant par la distribution, le contrôle des inventaires, la conception des produits et la planification financière.

Dans le domaine de l'agriculture, permettez-moi de vous donner un exemple tiré de l'expérience de la Banque Royale elle-même. Nos agrologues utilisent maintenant des ordinateurs portatifs afin d'aider les fermiers à prévoir leur fonds de roulement en utilisant des projections de récoltes, le coût des intrants et les prix du marché mondial. Ces

projections qui demandaient autrefois des heures sont maintenant faites en quelques secondes, grâce aux données informatisées modernes sur les prix des denrées sur les marchés à terme, les tendances météorologiques et ainsi de suite.

Le progrès technologique permet peut-être de créer de nouveaux services d'information et des bases de données économiques. Mais leur utilité dépend d'un accès ininterrompu assuré aux usagers. Prenons le cas de la société Dresser Industries. Vous vous rappelez peut-être qu'après l'imposition de la loi martiale en Pologne, le gouvernement des États-Unis a interdit à la filiale française de cette entreprise de fournir du matériel ou de la technologie pour le pipeline de gaz trans-sibérien. On peut imaginer ce qu'il est advenu de la valeur économique et de la réputation de Dresser France, dès le moment où cette société n'a plus eu accès aux connaissances spécialisées et à l'information.

En l'absence d'ententes internationales assurant un accès ininterrompu aux services d'information, les entreprises doivent se mouvoir dans un environnement incertain. Il existe un danger que certains pays décident unilatéralement de restreindre les catégories d'information qui peuvent être envoyées, traitées ou emmagasinées à l'étranger. Il pourrait en résulter un éventail de règles et de règlements restrictifs, allant des barrières tarifaires et non tarifaires aux tentatives gouvernementales en vue d'enregistrer, de taxer et de contrôler toutes les banques de données. Cette menace du protectionnisme de l'information est plus grande pour le Canada, avec son marché intérieur relativement restreint, qu'elle ne l'est pour les plus grandes nations et les blocs commerciaux.

Un autre motif d'incertitude vient du fait qu'il est possible que certains États européens se livrent au protectionnisme commercial, sous couvert de protection des renseignements personnels. Les autorités responsables de la réglementation doivent maintenir une nette distinction entre le droit à la protection des renseignements personnels et les problèmes commerciaux. La protection des renseignements personnels est déjà suffisamment complexe et exigeante, sans qu'on y mêle également les problèmes économiques.

Le concept de protection des renseignements personnels a pris une grande ampleur. Du point de vue des banquiers, il s'agit d'une évolution intéressante. Traditionnellement, ceux-ci ont dû satisfaire les attentes élevées du public à l'égard de deux aspects de la protection des renseignements personnels:

Le premier de ces aspects est la "sécurité". Les coffres bancaires se doublent maintenant de "gardiens" informatisés interdisant aux personnes non autorisées l'accès aux bases de données.

Le deuxième aspect est la "confidentialité": les banquiers, tout comme les médecins et les avocats, sont les gardiens des renseignements au sujet de leurs clients. Ils sont tenus à l'obligation contractuelle de ne les divulguer à des tiers que dans certaines circonstances définies très restrictivement, principalement dans les cas où le client y consent et lorsqu'ils y sont obligés par la loi.

Pour toutes ces raisons, la Banque Royale a proposé et a activement encouragé l'idée d'une entente sectorielle entre le Canada et les États-Unis portant sur ce que nous appelons "les services informatiques partagés", un accord bilatéral qui pourrait servir de modèle à une libéralisation multilatérale ultérieure. Notre proposition a un double objectif. L'un d'entre eux consiste à établir des règles d'échange mutuellement acceptables, régissant l'accès aux marchés pour les fournisseurs canadiens et ceux des États-Unis, ainsi que l'accès aux services informatiques pour les utilisateurs canadiens et ceux des États-Unis. L'autre objectif consiste à harmoniser la protection des renseignements personnels dans les deux pays. Je viens de commenter les problèmes économiques et commerciaux; passons maintenant à la protection des renseignements personnels.

Une mosaïque internationale de régimes de protection des renseignements personnels pourrait avoir des conséquences économiques sensiblement semblables à celles qu'auraient des restrictions pures et simples sur le commerce et les échanges d'information. Les entreprises devraient alors supporter les frais et l'inefficacité résultant d'une réglementation variant d'un pays à l'autre; ou, ce qui serait même pire, certains gouvernements risquent d'insister pour que tous les renseignements personnels soient traités dans des banques de données nationales, au motif que les autres pays n'offrent pas une protection équivalente aux renseignements personnels. À l'exception de l'Europe, les règles internationales sur la protection des renseignements personnels sont incertaines. Les flux d'information peuvent être interrompus de façon arbitraire et imprévisible.

Toutefois, le concept de "protection des renseignements personnels" va maintenant bien au-delà de la "sécurité" et de la "confidentialité". Il est perçu comme un ensemble complet de droits qui confèrent aux individus un certain contrôle sur les renseignements personnels qui les concernent, non seulement sur la façon dont ces renseignements sont communiqués, mais aussi sur la façon dont ils sont colligés, traités, utilisés, vérifiés et corrigés en cas d'erreur.

Les banques sont des entreprises qui utilisent largement l'information, qui doivent obtenir des renseignements personnels confidentiels dans le cadre de leurs activités et qui doivent s'assurer la confiance du public pour pouvoir les poursuivre. Nous sommes pleinement conscients du fait que nos principes et nos pratiques à l'égard de l'information doivent refléter le concept moderne de "protection des renseignements personnels". L'expérience que nous avons acquise en matière de "sécurité" et de "confidentialité" constitue une fondation solide sur laquelle nous appuyer.

Il est essentiel, non seulement que les renseignements personnels soient protégés et que la confiance du public soit maintenue mais, pour les raisons économiques que j'ai commentées, que les exigences en cette matière des diverses nations soient raisonnablement uniformes.

De toute évidence, les nombreuses lois sur la protection des renseignements personnels adoptées en Europe et en Amérique du Nord ne sont pas parfaitement uniformes. Les principales différences portent sur les

méthodes d'application et la portée de la réglementation, si elle s'applique seulement, par exemple, au secteur public ou également au secteur privé, ou aux systèmes d'information automatisés ainsi qu'aux dossiers manuels.

Il est toutefois un fait plus important que ces différences, soit que la législation existante reflète la même préoccupation fondamentale: donner à l'individu un contrôle raisonnable sur les renseignements personnels qui le concernent, et imposer les règles correspondantes aux gouvernements et aux sociétés.

Il serait peut-être irréaliste de vouloir établir, à l'extérieur du Canada, un système permettant d'uniformiser parfaitement toutes les lois sur la protection des renseignements personnels, mais on peut raisonnablement identifier leurs points communs. Comme je l'ai déjà suggéré, c'est là que réside la valeur des lignes directrices de l'O.C.D.E. Elles établissent des principes fondamentaux de la protection des renseignements personnels, qui pourraient être considérés comme le dénominateur commun des codes de protection des renseignements personnels dans de nombreux pays, qu'ils soient imposés par une loi, aux termes d'une politique de réglementation, ou volontairement.

Dans ces circonstances, on doit se poser les questions pratiques suivantes: les pays peuvent-ils "harmoniser" leurs principes directeurs sur la protection des renseignements personnels, si leur cadre réglementaire est différent? Les individus peuvent-ils être certains que

les renseignements personnels à leur sujet seront protégés à l'étranger comme ils le sont dans leur propre pays? Ma réponse à ces deux questions est un "oui" nuancé.

La première réserve tient à l'attitude des gouvernements. Comme je l'ai avancé, ceux-ci doivent maintenir une nette distinction entre la protection des renseignements personnels et les problèmes commerciaux. C'est là une condition essentielle de l'harmonisation.

Mon autre réserve est due à l'attitude du secteur privé. Le milieu des affaires doit réaliser que des codes rigoureux et uniformes de protection des renseignements personnels peuvent largement contribuer à réduire la nécessité d'une réglementation gouvernementale. Cela confirmera également dans l'esprit des citoyens que la transmigration des données n'est pas un phénomène menaçant.

Évidemment, aucun gouvernement n'abandonnera ses responsabilités en cette matière ni ne laissera le secteur privé décidé de quelle façon, et dans quelles conditions, les renseignements personnels pourront être transmis au-delà des frontières. Mais cela allègera les pressions politiques incitant les gouvernements à prendre "les premiers" l'initiative d'une législation sur la protection des renseignements personnels ... si les sociétés prennent les mesures nécessaires pour étoffer l'embryon des lignes directrices de l'O.C.D.E. ... si les sociétés multinationales commencent à adopter des codes applicables dans l'ensemble de l'industrie, ou entre les sociétés ... si les compagnies démontrent au public qu'elles prennent des

mesures spécifiques afin de réduire les risques d'un traitement inapproprié des renseignements personnels dans les bases de données et les centres de traitement étrangers. De telles mesures de la part du secteur privé constituent la base fondamentale qui permettra à l'avenir au gouvernement d'harmoniser les lois d'une façon plus formelle.

Le secteur privé multinational ne devrait pas sous-estimer son influence. Il fonctionne depuis longtemps dans différents environnements politiques, juridiques et réglementaires. Il possède également les connaissances en matière de technologie de l'information, dont les gouvernements ont besoin pour élaborer des principes directeurs viables.

Les mesures prises par le gouvernement afin d'harmoniser la protection des renseignements personnels sont les plus efficaces lorsqu'elles sont prises par des pays voisins, possédant des systèmes juridiques semblables. Nous constatons déjà ce phénomène en Europe. Il me semble que le Canada et les États-Unis pourraient suivre cet exemple et négocier une "entente modèle" nord-américaine portant sur des sujets comme le droit de rechercher l'information, le droit à une protection équivalente, l'exécution réciproque des jugements et des procédures mutuellement acceptées permettant de déterminer la compétence des tribunaux lorsque le litige oppose les citoyens des deux pays.

Cependant, le Canada ne peut négocier des ententes internationales si le gouvernement fédéral et les provinces n'adoptent pas une approche uniforme à l'égard de la protection des renseignements personnels.

Nous ne pouvons tout simplement nous présenter à la table de négociations avec des gouvernements pouvant prendre de deux à onze orientations différentes sur un problème aussi fondamental de droits humains.

Comme je l'ai déjà mentionné, l'uniformité répond également à un impératif purement intérieur. Le Canada devrait préserver son marché commun dans le domaine des flux et des services d'information. Les gouvernements devraient songer aux conséquences financières de l'établissement de systèmes réglementaires différents. Même aujourd'hui, des différences mineures dans des domaines tels que le calcul des taux d'intérêt et les exigences relatives aux rapports financiers peuvent obliger les sociétés à développer des programmes informatiques et des applications de logiciel totalement différentes pour diverses juridictions. Le même problème pourrait se présenter si les exigences relatives à la protection des renseignements personnels différaient d'un gouvernement à l'autre.

Étant un homme d'affaires, je n'ai pas d'idée très arrêtée sur la délimitation précise des compétences fédérale/provinciale en matière de protection des renseignements personnels. Ce qui est extrêmement important toutefois, c'est que les gouvernements du Canada commencent par "s'entendre pour s'entendre" sur un code national uniforme du droit à la protection des renseignements personnels pour tous les Canadiens. J'ai pu constater par expérience que les Canadiens s'attendent à bénéficier de droits identiques à la protection des renseignements personnels, quel que soit l'endroit où ils vivent, ou l'endroit où ils pourraient déménager un jour au Canada. Si ma perception est exacte, les gouvernements auraient politiquement intérêt à adopter une approche commune.

Si l'on peut s'entendre sur les droits à la protection des renseignements personnels, nous pourrions alors nous pencher sur la question des rôles respectifs d'Ottawa, des provinces, des territoires et du secteur privé pour assurer le respect de ces droits.

Dans leurs tentatives en vue d'établir un cadre réglementaire uniforme, tous les gouvernements devraient être conscients du rôle que peut jouer le secteur privé. Les sociétés, les associations industrielles et les autres groupes du secteur privé peuvent aider le gouvernement en faisant en sorte que les principes fondamentaux de la protection des renseignements personnels soient appliqués de façon efficace et uniforme dans tout le pays. Une autoréglementation efficace entièrement intégrée aux mesures prises afin d'assurer le respect des droits à la protection des renseignements personnels peut aider les autorités fédérale et provinciales à atteindre un consensus. Pour être efficace, l'autoréglementation doit refléter un consensus national sur la protection des renseignements personnels.

La protection des renseignements personnels est une question importante, qui doit être débattue en profondeur par toutes les parties concernées. Grâce à cette conférence, nous avons pu amorcer le débat. Je vous remercie de m'avoir permis d'y participer.

DOCUMENT: 870-123/017

INTERPROVINCIAL CONFERENCE ON PRIVACY:
INITIATIVES FOR 1984 (SYMPOSIUM)

Notes for a Presentation

By

Caroline Pestieau
Commissioner
Quebec Access to Information Commission



Toronto, Ontario
May 23-24, 1984

PRIVACY: SOME PRACTICAL SOLUTIONS

In the next few minutes, I will be discussing the main data protection features of Quebec's Freedom of Information and Protection of Privacy Law. Before I begin, I should like to explain my understanding of the «practical solutions» in the title of our panel today.

More than two dozens countries, states and provinces have adopted Data Protection laws. In each case, their lawmakers have had to choose from a menu of principles, institutional arrangements, procedures and definitions. In this presentation, I will be looking at the strategic choices Quebec's National Assembly made when it adopted An Act respecting Access to documents held by public bodies and the Protection of personal information in June, 1982. I will devote most of my time to highlighting the essential characteristics of our law in the Data Protection field, after which I will mention one or two of the strategic options facing the body responsible for supervising the implementation of the act, the Quebec Access to Information Commission, of which I am privileged to be a member.

There therefore won't be much in the way of nuts and bolts of individual cases in this talk. However, on July 1st, when the main provisions of our law come into force, we will deal with the individual problems and cases which arise according to the principles and procedures established by the law. In this sense, my presentation is practical. I am talking about rights and obligations embodied, since June, 1982, in legal and institutional machinery. Since Quebec is so far the only Canadian province to have full-fledged data protection legislation, I believe that this exercise may be worthwhile to others who are considering what type of machinery to adopt.

The Access Law

I will be referring to the Quebec law by its short title as the Access Law. Despite this somewhat confusing nomenclature, the part of the law which concerns us today is essentially a Fair Information Practices Act. It shares a number of features with all such acts. First of all, it states that nominative, that is personal, information is confidential unless the person the information concerns authorizes its disclosure. As corollaries to this principle the Access Law requires that only necessary personal information be collected, that the agency representative who collects the information inform the person concerned or data subject of the purpose for which it is being collected and to whom it will be released. The collecting or holding agency is

responsible for the accuracy of the information it holds and for its destruction when it is no longer needed. The data subject has free access to his/her personal data file. He/she can request corrections if the information on file is inaccurate, incomplete or equivocal or if the collection was illegal. In all such instances the burden of proof rests with the agency.

What is special about Quebec's Data Protection Law? In opting for certain mechanisms, principles and procedures, rather than for others, the Quebec lawmakers moulded the law in a particular way. I should like to review five of its principal characteristics with you: the legal context, the law's coverage, its attitude to Government as a repository of personal data, its creation of a supervisory commission and its detailed nature.

The legal context

The Quebec law guarantees both freedom of information and data protection in one act. Freedom of information and privacy are the subjects of chapters II and III respectively, while the general provisions of the other chapters apply to both these rights. All three Commissioners are responsible collectively and individually for both sets of rights, although, as we shall see later, the

Commission's mandate is wider in the case of data protection than in the case of access to administrative documents. There should therefore be no downgrading of one set of rights with the respect to the other.

The Access Law is a fundamental law which takes precedence over all subsequent legislation unless a new law expressly states that it applies notwithstanding the Access Law. One of the Commission's tasks is to examine existing legislative provisions which are inconsistent with the Access Law and recommend amendments in one law or in the other. In the absence of harmonizing amendments, inconsistent provisions are automatically suspended three years after proclamation of the Access Law, that is to say, in October, 1986.

The Access Law also has its own sunset clause. Five years after its proclamation, the Quebec Access to Information Commission has to report to the Government on the way in which it has been working and on the advisability of maintaining or amending it. The Government tables this report in the National Assembly which decides on the law's future within the following year.

Coverage

The Quebec Law only applies to the public sector but it gives that sector a very wide extension. Whereas the federal law applies to about 130 agencies, the Access Law covers about 3 600, including towns and cities, school boards, hospitals, universities and crown corporations. These agencies cannot ignore the law since in each the person exercising the highest authority automatically becomes the access and privacy coordinator unless he/she delegates this responsibility to another management person. Although the law does not cover the private sector, it does regulate the flow of personal data between public and private agencies. For the sake of completeness, I should also mention that the Access Law applies to both manual and automatically processed files.

A particular characteristic of the Quebec Access Law is its coverage of so called «confidential» files. The Government can authorize the setting up (or the continuation) of a confidential file by an order-in-council specifying the kind of information to be filed, the use to which it is to be put, security and conservation measures to be taken and the categories of people having access to it. Before making or amending such an order, the Government has to obtain the opinion of the Commission and the order itself and the opinion are tabled in the National Assembly.

Naturally, the people concerned do not have access to their records in confidential files, but the Commissioners do. They can investigate a confidential file to determine whether or not the personal information it contains was entered and used in accordance with the order tabled by the Government.

Government as a repository of personal information

Under this heading, I should like to say a few words about the way in which the Access Law considers public bodies as recipients and repositories of citizens' personal data. It is clear from the law that a citizen who provides information to a public agency, usually as a condition for receiving a service, does not yield it up to a monolithic Administration which can use it in whichever branch of its activities it pleases. Data is collected by one of the three thousand six hundred departments, hospitals, crown corporations or other bodies not by the Government of Quebec. Thus data collected by a particular hospital is not necessarily available to the Department of Health, data on eligibility for welfare is not automatically available to educational officials screening bursary applications and so on. One agency can only release data to another under a written agreement tabled in the National Assembly to which the Commission's evaluation of the proposed transfer is annexed. Thus everyone can find out to whom the agency which originally collected his/her data may be releasing it.

The Access to Information Commission

I now come to the fourth and one of the most important characteristics of the Quebec Access Law - its creation of a special agency to supervise implementation of the law. In contrast to the situation in the United States where citizens themselves have to take legal action if their freedom of information and protection of privacy rights are not respected, Quebec has set up a three-member commission to make sure that the new rights it has accorded are respected.

The Commission is a hybrid body with tasks akin to those of an administrative tribunal, a regulatory agency and an advisory body. Acting as a tribunal, its first duty is to hear requests for review of administrative decisions regarding access to public documents and access to personal data files, as well as requests for the correction of such files by the persons they concern. The Commission's decisions on questions of fact within its competence are final and it can issue a binding order: «to release a document or part of a document, refrain from doing so, correct, complete, clarify, update or delete any nominative information, or discontinue the use or the release of nominative information».

While its duties on the freedom of information side are essentially limited to reviewing agency decisions, the Commission also acts as a supervising body dealing with personal data. Agencies have to declare all their data files to the Commission which draws up the declaration form. The Commission draws on these declarations to publish and update an index of all personal information files maintained by public sector agencies. It is responsible for authorizing the release of personal data for research purposes and has various other administrative functions.

The Commission's third major task is to give the Government its opinion on a number of questions, the most important of which have already been mentioned - data linkage agreements for the transfer of personal information between agencies and the creation or modification of confidential files. With the respect to the former, it is worth mentioning that the Access Law does not set out principles to guide inter-agency data exchanges, such as routine or compatible use, so the Commission has had to develop its own thinking in offering advice on proposed inter-agency data releases.

The members of the Commission are appointed by the National Assembly for a five-year term of office and can only be dismissed by a two-thirds majority of the Assembly. Their annual reports, and any special reports they feel the need to present on non-compliance with the act, are examined by the Assembly within a statutory time period. The Commission's independence vis-à-vis the administration in general is thus based on its relationship with the Legislature. The law does allow the Government to use an executive veto against an access decision of the Commission, in which case the Commission will have to rely on the credibility it has established with the media and public opinion to maintain its independence. This veto, however, mainly applies to the freedom of information part of the law. Apart from a possible application to a data subject's access to his/her file, the Commission's powers in the data protection area are unaffected by this form of executive control.

The Access Law's precision

The last characteristic I want to discuss with you is a qualitative one that I have not been able to put a name to. It concerns the degree of elaboration in the Access Law. Quebec lawmakers obviously wanted to avoid problems which had arisen in other countries as a result of administrative inertia or of imprecise drafting. As a result they included a number of detailed requirements some of which go further than those in most other data protection legislation. One example is an agency's obligation to record each non-routine

consultation of a personal record file and to make this record available to the data subject. This in turn leads to a definition of types of employees who may consult the file on a routine as opposed to a non-routine basis. In their determination to avoid the ambiguities which have cropped up elsewhere, the authors tried to plug all the loopholes and as a result have produced an elaborate set of rights and obligations.

On the one hand this makes the work of the Commission easier. Many of the problems which would have inevitably surfaced sooner or later are already identified and can be worked on. On the other hand, there is a danger of the Access Law giving rise to an arcane bureaucratic set of procedures which lose contact with the fundamentals of data protection. The members of the Commission are well aware of this danger and intend to avoid getting bogged down in bureaucratic hassles while using the detailed provisions of the law to their best advantage.

Strategic choices facing the Commission

I have just mentioned one important choice in referring to the Commission's determination to prevent the freedom of information and data protection procedures from becoming overly bureaucratized.

I would like to conclude by raising two other questions which are among the many that the Commission will have to address as it carries out its mandate. The first concerns the right balance between concentrating on responding to individual citizens' requests regarding their own personal files - access, correction, conservation, etc. - and allocating resources to auditing agency files in order to insure compliance with the law. The two activities are obviously closely interconnected. Individual requests may signal the need for an audit, while an efficient audit will act as a preventive measure eliminating abuses about which citizens might have complained. While there is no question whatsoever of downgrading citizens' requests, experience elsewhere has shown that these are often insufficient to insure agency compliance which requires, in addition, active encouragement and monitoring.

A second strategic option is that of the Commission's stance vis-à-vis agency file holders. When not acting as an administrative tribunal, the Commission could choose to work with the file holders in the agencies in developing acceptable standards for collecting and managing personal information as the German Federal Commission appears to have done. Or it could keep its distance in policing personal data processing according to the principles of the law.

Obviously that can be no hard and fast, a priori, answers to either of these questions. I have mentioned them in order to share with you some of the challenges a law such as the Access Law, which creates new rights, obligations and institutions, inevitably sets for those who have to oversee its implementation. The Access to Information Commission is at the moment a hive of reflection and activity in preparation for the proclamation of the main articles of the law on July 1st. In the course of responding to the diverse situations which will arise, we hope to make the choices most appropriate to the law's objectives which are to insure freedom of information and protection of personal data without depriving Quebecers of a responsible and efficient administration.

CA1
Z2
- C52

DOCUMENT: 870-123/017

CONFERENCE INTERPROVINCIALE SUR LA PROTECTION
DES RENSEIGNEMENTS PERSONNELS: MESURES POUR 1984 (COLLOQUE)

Notes en vue d'une allocation

prononcée par

Caroline Pestieau

Commissaire

Commission d'accès à l'information du Québec



Toronto (Ontario)
les 23 et 24 mai 1984

PROTECTION DES RENSEIGNEMENTS PERSONNELS:

QUELQUES SOLUTIONS PRATIQUES

Au cours des prochaines minutes, j'aimerais analyser les principaux éléments qui, dans la Loi québécoise sur l'accès à l'information et sur la protection de la vie privée portent sur la protection des données personnelles. Avant de commencer, j'aimerais expliquer ce que j'entends par les «solutions pratiques» qui font l'objet de notre discussion d'aujourd'hui.

Plus d'une vingtaine d'États et provinces ont adopté des lois sur la protection des données. Dans chaque cas, les législateurs durent choisir entre un nombre considérable de principes, de modalités institutionnelles, de procédures et de définitions. Lors de cet exposé, j'examinerai les choix stratégiques que l'Assemblée nationale du Québec a faits lorsqu'elle a adopté, en juin 1982, la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels. Je ferai surtout ressortir les principales caractéristiques de notre loi dans le domaine de la protection des données. Je vous parlerai également d'un ou de deux des choix stratégiques qui s'offrent à l'organisme chargé de surveiller la mise en oeuvre de la loi, la Commission d'accès à l'information du Québec, dont j'ai le privilège d'être membre.

Il ne sera donc pas question dans mon exposé des points de détail ni de cas individuels. Toutefois, lorsque les principales dispositions de notre loi entreront en vigueur le 1er juillet, nous devrons traiter, selon les principes et les règles établis par cette loi, les problèmes et les cas individuels qui surviendront. En ce sens, mon

exposé est pratique. Je parlerai des droits et des obligations que le législateur a traduits depuis juin 1982 dans des mécanismes juridiques et institutionnels. Puisque, jusqu'ici, le Québec est la seule province canadienne à avoir adopté une loi sur la protection des données personnelles, je crois que cette analyse sera utile à ceux qui se demandent quel genre de mécanisme adopter chez eux.

La Loi sur l'accès

J'utiliserai le titre abrégé de la loi québécoise, soit la Loi sur l'accès. Dans les circonstances présentes, cette appellation peut paraître trompeuse. En fait, le volet de la loi auquel je réfère reprend essentiellement les exigences de ce qu'on convient d'appeler un «Fair Information Practices Act». D'abord, il y est prévu que les renseignements nominatifs, c'est-à-dire personnels, sont confidentiels à moins que la personne concernée n'autorise leur divulgation. Comme corollaires à ce principe, la Loi sur l'accès prévoit que seuls les renseignements personnels nécessaires peuvent être recueillis, et que le représentant de l'organisme qui les recueille doit informer la personne concernée de la raison pour laquelle les renseignements sont recueillis et à qui ils seront communiqués. L'organisme qui recueille ou qui détient les renseignements est responsable de leur exactitude et de leur destruction une fois qu'ils ne sont plus utiles. La personne concernée a le droit de consulter son dossier personnel. Elle peut exiger que des rectifications y soient apportées si les renseignements sont inexacts, incomplets ou équivoques, ou si leur collecte n'était pas autorisée par la loi. Dans tous ces cas, le fardeau de la preuve incombe à l'organisme.

Qu'a de spécial la loi du Québec sur la protection des données? En choisissant certains mécanismes, principes et procédures plutôt que d'autres, le législateur du Québec a façonné la loi d'une manière

particulière. J'aimerais analyser avec vous cinq des principales caractéristiques de cette loi: son régime juridique, son champ d'application, sa vision du gouvernement en tant que dépositaire de données personnelles, sa commission de surveillance et sa nature détaillée.

Le régime juridique

Le Québec garantit, dans une seule loi, l'accès à l'information et la protection des renseignements personnels. Ces deux volets de la Loi sont traités dans les chapitres II et III respectivement. Les dispositions générales, quant à elles, sont réparties dans les autres chapitres et s'appliquent à ces deux volets. Les trois commissaires doivent veiller au respect des deux droits, même si, comme nous le verrons plus tard, la portée du mandat de la Commission est plus vaste dans le cas de la protection des données que dans celui de l'accès aux documents administratifs. On ne pourra donc pas minimiser l'importance d'un volet de la loi par rapport à l'autre.

La Loi sur l'accès est une loi fondamentale qui a préséance sur toutes les lois ultérieures à moins qu'il ne soit précisé expressément, dans une nouvelle loi, qu'elle s'appliquera par dérogation à la Loi sur l'accès. D'autre part, une des tâches de la Commission consiste à examiner les dispositions législatives antérieures à la Loi sur l'accès qui sont incompatibles avec celles de la Loi sur l'accès et à faire les modifications qui s'imposent. Faute de modification, les dispositions inconciliables seront automatiquement inopérantes trois ans après l'entrée en vigueur de la Loi, c'est-à-dire en octobre 1986.

La Loi sur l'accès a également sa propre clause crépusculaire. Cinq ans après l'entrée en vigueur de la Loi, la Commission d'accès à l'information du Québec doit faire rapport au gouvernement sur sa mise

en oeuvre et sur l'opportunité de la maintenir ou de la modifier. Le Gouvernement déposera ce rapport à l'Assemblée nationale qui doit, dans un délai d'un an, décider de l'avenir de la loi.

Le champ d'application

La loi du Québec ne s'applique qu'au secteur public, mais elle accorde à cette expression un sens très large. Alors que la loi fédérale s'applique à environ 130 organismes, la Loi sur l'accès en vise pour sa part quelque 3 600, y compris les villes et municipalités, les commissions scolaires, les hôpitaux, les universités et les sociétés d'État. Ces organismes ne peuvent passer outre à la loi car, dans chacun, la personne exerçant la plus haute autorité devient la personne responsable de l'accès aux documents et de la protection des renseignements personnels à moins qu'elle ne délègue cette responsabilité à un autre membre de son personnel de direction. La loi ne s'applique pas au secteur privé, mais elle régit l'échange de renseignements personnels entre les organismes publics et privés. Pour épuiser le sujet, je devrais ajouter que la Loi sur l'accès s'applique aux dossiers manuels et informatisés.

Un des traits particuliers de la Loi sur l'accès du Québec est la façon dont elle traite les fichiers dits «confidentiels», c'est-à-dire des fichiers de renseignements servant à la détection ou à la répression des crimes ou des infractions aux lois. Le Gouvernement peut, par décret, autoriser l'établissement (ou le maintien) d'un fichier confidentiel en précisant le type de renseignements qu'il peut contenir, l'usage qui peut en être fait, les mesures de sécurité et de conservation à prévoir ainsi que les catégories de personnes qui peuvent y avoir accès. Avant de prendre ou de modifier pareil décret, le Gouvernement doit demander l'avis de la Commission et déposer le décret et l'avis à l'Assemblée nationale.

Naturellement, les personnes concernées n'ont pas accès aux fichiers confidentiels. Mais les commissaires peuvent les examiner. Ils peuvent vérifier un fichier confidentiel afin de déterminer si les renseignements personnels qu'il renferme ont été inscrits et utilisés conformément au décret pris par le Gouvernement.

Le Gouvernement en tant que dépositaire de renseignements personnels

Ici j'aimerais dire quelques mots sur la façon dont les organismes publics sont vus par la loi dans leur rôle de destinataire et de dépositaire de renseignements personnels sur les citoyens. Selon les termes de la loi, il est évident qu'un citoyen qui fournit un renseignement personnel à un organisme public, habituellement en vue de recevoir un service, ne le cède pas à une administration monolithique qui peut s'en servir comme il lui plaît dans toutes les branches de ses activités. Les renseignements personnels sont recueillis par un des 3 600 ministères, hôpitaux, sociétés d'État ou autres organismes, et non par le Gouvernement du Québec. Ainsi les renseignements recueillis par un hôpital ne sont pas tous transmis d'office au ministère des Affaires sociales, ceux qui touchent l'admissibilité au Bien-Être social ne sont pas automatiquement accessibles aux fonctionnaires qui examinent les demandes de bourses d'étude et ainsi de suite. En règle générale, un organisme ne peut communiquer des renseignements à un autre organisme qu'en vertu d'une entente écrite approuvée par le Gouvernement. La Commission est appelée à donner son avis sur l'entente qui est déposée, ainsi que l'avis de la Commission, à l'Assemblée nationale. De cette façon, un citoyen peut savoir à qui un organisme qui a recueilli des renseignements à son sujet peut les avoir transmis.

La Commission d'accès à l'information

Nous voici maintenant au quatrième trait caractéristique de la Loi sur l'accès du Québec, l'un des plus importants d'ailleurs, soit la création d'un organisme spécial chargé de surveiller la mise en oeuvre de la loi.

Contrairement à la situation qui prévaut aux États-Unis, où les citoyens doivent eux-mêmes prendre une action en justice si leurs droits d'accès à l'information et de protection des renseignements personnels ne sont pas respectés, le Québec a mis sur pied une commission composée de trois membres et chargée de faire en sorte que les nouveaux droits accordés soient respectés.

La Commission est un organisme hybride dont les tâches ressemblent à la fois à celles d'un tribunal administratif, d'un organisme de réglementation et d'un conseil consultatif. À titre de tribunal, sa première tâche consiste à entendre les demandes de révision des décisions administratives concernant l'accès à des documents publics et à des fichiers de renseignements personnels, ainsi que les demandes de rectification de ces fichiers par les personnes concernées. Les décisions de la Commission sur des questions de fait sur lesquelles elle a compétence sont finales. De plus, la Commission a les pouvoirs nécessaires pour ordonner à un organisme public «de donner communication d'un document ou d'une partie de document, de s'abstenir de le faire, de rectifier, compléter, clarifier, mettre à jour ou effacer tout renseignement nominatif ou de cesser un usage ou une communication de renseignements nominatifs».

En ce qui concerne le volet de l'accès à l'information, les fonctions de la Commission sont essentiellement limitées à la révision des décisions prises par les organismes. Mais en ce qui a trait aux renseignements personnels, la Commission agit également à titre d'organisme de surveillance. Les organismes doivent déclarer à la Commission, en utilisant un formulaire qu'elle a préparé, chacun des fichiers de renseignements personnels qu'ils détiennent. À partir de ces déclarations, la Commission publie et tient à jour un répertoire de tous les fichiers personnels détenus par les organismes publics. La Commission a aussi divers pouvoirs administratifs, dont le devoir d'autoriser la communication de renseignements personnels à des fins de recherche.

La troisième grande tâche de la Commission en est une de conseiller le Gouvernement sur certaines questions, dont les plus importantes ont déjà été mentionnées. Il s'agit des ententes de transfert de renseignements personnels entre organismes qui peuvent prendre la forme de couplages de fichiers et l'établissement ou la modification de fichiers confidentiels. Pour ce qui est des ententes, il convient de mentionner que la Loi sur l'accès n'établit aucun principe général, comme par exemple l'acceptation d'une utilisation courante ou compatible pour évaluer la pertinence d'un échange de renseignements entre deux organismes. Suite à une étude approfondie de ce secteur, la Commission a établi des critères d'évaluation des transferts de renseignements personnels.

Les membres de la Commission sont nommés par l'Assemblée nationale pour un mandat de cinq ans et ne peuvent être destitués que par une décision d'au moins les deux tiers de l'Assemblée. Les rapports annuels de la Commission, et tous les rapports spéciaux qu'elle juge nécessaire de présenter concernant le non respect de la Loi sont examinés par l'Assemblée dans un délai prévu par la loi. L'indépendance de la Commission par rapport à l'administration est donc fondée sur ses rapports avec l'assemblée législative. La loi permet au Gouvernement d'opposer un veto à une décision rendue par la Commission relativement à une demande d'accès, et cette dernière devra alors compter sur la crédibilité dont elle jouit auprès des médias et du public pour conserver son indépendance. Toutefois, ce veto s'applique surtout à la partie de la loi qui traite de l'accès à l'information. Sauf dans la mesure où il peut nier le droit d'accès d'une personne au fichier personnel la concernant, ce contrôle exécutif ne porte pas atteinte aux pouvoirs de la Commission dans le domaine de la protection des renseignements personnels.

Précision de la Loi sur l'accès

Le dernier trait caractéristique que je voudrais analyser avec vous est qualitatif et je n'ai pu le doter d'une appellation précise. Il s'agit de la minutie avec laquelle la loi a été rédigée. En effet, le législateur québécois a manifestement voulu éviter les problèmes qui sont survenus dans d'autres pays en raison de l'inertie administrative ou d'un libellé imprécis. Par conséquent, il a inclu des exigences dont certaines vont plus loin que la plupart des autres lois sur la protection des renseignements personnels. Par exemple, un organisme est obligé d'enregistrer chaque consultation non habituelle d'un fichier de renseignements personnels afin de permettre à la personne faisant l'objet des renseignements de savoir qui a consulté son dossier. Il s'ensuit une définition des employés qui peuvent consulter le fichier dans l'exercice de leurs fonctions sans être tenus de s'enregistrer. Déterminés à éviter les ambiguïtés qui sont survenues ailleurs, les auteurs ont tenté de combler toutes les lacunes et, partant, ont créé un ensemble complexe de droits et d'obligations.

D'une part, la tâche de la Commission est ainsi facilitée. Beaucoup des problèmes qui seraient inévitablement survenus tôt ou tard sont déjà identifiés et appellent une résolution. D'autre part, il y a un risque que la Loi sur l'accès ne donne lieu à un train de mesures bureaucratiques complexes qui feraient perdre de vue les principes essentiels de la protection des données personnelles. Les membres de la Commission sont conscients de ce danger. Ils ont l'intention de ne pas se laisser enliser dans les chinoïseries administratives et de faire le meilleur usage possible des dispositions détaillées de la loi.

Choix stratégiques s'offrant à la Commission

Je viens de mentionner un choix important qu'a fait la Commission lorsqu'elle a décidé de faire en sorte que les procédures relatives à l'accès à l'information et à la protection des renseignements personnels ne soient pas assujetties à une bureaucratie trop envahissante.

Pour conclure, je voudrais soulever deux autres questions de fond qui se posent à la Commission. La première touche l'équilibre à établir entre l'attention accordée aux demandes individuelles des citoyens concernant leurs fichiers personnels - accès, rectification, conservation, etc. - et l'affectation de ressources à la vérification des fichiers des organismes afin de veiller à ce que la loi soit respectée. Il va sans dire que les deux activités sont étroitement reliées. Les demandes individuelles peuvent indiquer le besoin de vérification, tandis qu'une vérification efficace servira de mesure préventive afin d'éliminer les abus dont les citoyens pourraient se plaindre. Il n'est pas du tout question de minimiser l'importance des demandes des citoyens, mais l'expérience des commissaires dans d'autres pays a démontré que ces demandes ne suffisent souvent pas à faire en sorte que la loi soit respectée. Les organismes ont en outre besoin d'être activement encouragés et surveillés pour qu'ils modifient leurs pratiques pour les conformer à la loi.

Dans un autre ordre d'idées, la Commission fera un choix stratégique en arrêtant la nature de ses relations avec les détenteurs de fichiers. Lorsqu'elle n'agit pas à titre de tribunal administratif, la Commission pourrait opter de travailler de concert avec les détenteurs de fichiers dans les organismes à l'élaboration de normes acceptables de collecte et de gestion des renseignements personnels. C'est la pratique de la Commission fédérale de protection de données personnelles en Allemagne. Ou bien elle pourrait garder ses distances et n'intervenir auprès des organismes que pour surveiller leur traitement des renseignements personnels selon les principes de la loi.

Il va sans dire que, a priori, on ne peut déterminer quels choix sont les meilleurs. J'en ai fait mention afin de vous faire connaître le genre de défis que pose inévitablement à ceux qui doivent en surveiller la mise en oeuvre d'une loi comme celle sur l'accès qui crée de nouveaux droits, de nouvelles obligations et de nouvelles institutions. La Commission d'accès à l'information est actuellement une ruche de réflexion et d'activités en prévision de l'entrée en vigueur des principaux articles de la loi, soit le 1er juillet prochain. Pour répondre aux diverses situations qui surviendront, nous espérons faire les choix les plus conformes aux objectifs de la loi qui consistent à assurer la liberté d'information et la protection des renseignements personnels sans priver les Québécois d'une administration responsable et efficace.

CA1
Z4
-C52

DOCUMENT: 870-123/C18

INTERPROVINCIAL CONFERENCE ON PRIVACY:
INITIATIVES FOR 1984 (SYMPOSIUM)

Notes for a Presentation

By

Douglas Smith
Assistant Deputy Minister
Communications Policy Branch
Department of Justice
Saskatchewan



Toronto, Ontario
May 23-24, 1984

PRIVACY IS NOT THE ISSUE THAT WE ARE DEALING WITH HERE AT THIS CONFERENCE. THE ELECTRONIC AGE HAS TAKEN US FAR BEYOND THE POINT OF THE OLD NOTIONS OF PRIVACY. PEOPLE TODAY HAVE TO ADOPT NEW ATTITUDES TOWARDS THIS SUBJECT; WE HAVE TO THINK IN TERMS OF NEW FORMS OF PRIVACY.

IT IS A GIVEN THAT FILES ARE HELD ON US; ON ANY ONE OF US WHO HAS EVER APPLIED FOR A MORTGAGE, FOR A VISA CARD, VISITED A DOCTOR, OPENED A BANK ACCOUNT, OR APPLIED FOR ANY ONE OF A THOUSAND CREDIT CARDS THAT ARE AVAILABLE. FOR THE CONVENIENCE OF GETTING ACCESS TO CREDIT, WE HAVE WITTINGLY - OR UNWITTINGLY - FORFEITED OUR PRIVACY.

FOR THE SPEED AND THE CONVENIENCE OF PULLING MONEY OUT OF WALLS WHEN BANKS ARE CLOSED, WE HAVE MADE OURSELVES NAKED. THERE ARE THOSE AMONG US - THE CIVIL LIBERTARIANS - WHO WOULD HAVE US RETURN TO THE DARK AGES, WHO WOULD HAVE US BELIEVE THAT IT IS WRONG THAT PEOPLE CAN COLLECT INFORMATION ON US. BUT YOU KNOW, ABSOLUTE PRIVACY IS A FAIRLY MODERN NOTION. IT DID NOT EXIST IN THE GREEK CITY STATE, AND IT DID NOT, AND STILL DOES NOT, EXIST IN COMMUNITIES OF 500. INFORMATION ABOUT PEOPLE LIVING IN SMALL COMMUNITIES IS VERY PUBLIC.

PAGE TWO

HOWEVER, WHAT DISTURBS PEOPLE TODAY IS THE ENORMOUS AMOUNTS OF INFORMATION THAT CAN BE STORED ABOUT THEM, THE KINDS OF INFORMATION, THE POSSIBLE MIS-USE OF THAT INFORMATION.

AND THIS IS WHAT THIS CONFERENCE IS ALL ABOUT. NOT PRIVACY, BUT THE MIS-USE OF INFORMATION. THIS IS THE REAL ISSUE. I PERSONALLY DO NOT MIND PEOPLE COLLECTING INFORMATION ON ME, BUT I ASK THEM NOT TO USE IT AGAINST ME MALICIOUSLY. THE QUESTION WE SHOULD SEEK ANSWERS TO IS: "ARE THERE WAYS OF CONTROLLING THE MIS-USE OF THIS INFORMATION? HOW CAN WE MAKE THE COLLECTORS OF INFORMATION ACCOUNTABLE?"

AND, THE ISSUE IS NOT NEW. SHAKESPEARE IN OTHELLO SAID:

"WHO STEALS MY PURSE, STEAL TRASH; TIS SOMETHING, NOTHING; TWAS MINE, TIS HIS, AND HAS BEEN SLAVE TO THOUSANDS; BUT HE THAT FILCHES FROM ME MY GOOD NAME, ROBS ME OF THAT WHICH NOT ENRICHES HIM, AND MAKES ME POOR INDEED."

NOW THEN, I AM SURE THEY DID NOT HAVE COMPUTERS IN SHAKESPEARE'S TIME, BUT HE TOO WAS SEIZED WITH THIS PROBLEM AS WE ARE IN SASKATCHEWAN. MY MINISTER, THE HONOURABLE J. GARY LANE, IS RESPONSIBLE FOR THE

PAGE THREE

PUBLICLY-OWNED TELEPHONE COMPANY, AND IS RESPONSIBLE FOR SASKCOMP, THE LARGEST COMPUTER INSTALLATION IN OUR PROVINCE.

MY MINISTER, MY GOVERNMENT, HAS A VERY REAL INTEREST IN ENSURING THAT THE TELEPHONE COMPANY SYSTEM IS NOT MIS-USED BY THOSE WHO WOULD TRANSPORT INFORMATION ACROSS THE SYSTEM. BUT, AT THE SAME TIME, THIS CONCERN IS TEMPERED BY THE KNOWLEDGE THAT TOO STRICT LEGISLATION OR SEVERE CONDITIONS ON USERS COULD STIFLE INITIATIVE TO INTRODUCE THE MYRIAD OF NEW TELECOMMUNICATIONS SERVICES NOW HERE AND ON THE HORIZON.

WE HAVE, AS MANY OF YOU MAY KNOW, THE LONGEST FIBRE OPTIC SYSTEM IN USE ANYWHERE IN THE WORLD IN SASKATCHEWAN. IT HAS TREMENDOUS CAPACITY, AND TREMENDOUS CAPABILITY FOR TWO-WAY INTERACTIVE DATA. WE HAVE ALSO IN THE PAST COUPLE OF YEARS BEEN GAINING INVALUABLE EXPERIENCE FROM INFORMATION SYSTEMS SUCH AS THE PATHFINDER TRIAL, AND THE AGRITEX SERVICE NOW IN USE.

PAGE FOUR

THE EXPERIENCE GAINED FROM THE PATHFINDER PROJECT HAS ASSISTED INFORMATION VENDORS AND SASKTEL IN DEVELOPING A MORE SOPHISTICATED VIDEOTEX ARRANGEMENT. THIS WILL ALLOW SUBSCRIBERS WHO HAVE THE APPROPRIATE EQUIPMENT TO ACCESS INFORMATION FROM ONE OF SEVERAL POTENTIAL DATA BASES THAT ARE LOCATED IN REMOTE AND INDEPENDENT LOCATIONS. THIS IS POSSIBLE BECAUSE SASKTEL NOW OWNS AND OPERATES A GATEWAY COMPUTER THAT BOTH FACILITATES UNITING USERS TO THE DATA BASE THEY REQUIRE AND ACCOMMODATES THE NECESSARY BILLING PROCESS. THE GATEWAY SERVICE WHICH SASKTEL OFFERS IS THE FIRST SUCH COMMERCIAL GATEWAY OF ITS KIND IN NORTH AMERICA. THE SERVICE IS CALLED AGRITEX AND THE DATA BASES THAT ARE AVAILABLE THROUGH IT ARE AVAILABLE THROUGH ONE OF TWO PROTOCOLS.

WHAT ARE THE IMPLICATIONS OF THESE TECHNOLOGIES AND SERVICES TO THE PUBLIC? THE FIRST IMPORTANT IMPLICATION IS THAT OUR TELECOMMUNICATIONS SERVICES ALLOW BUSINESS PEOPLE AND RESIDENTS OF SASKATCHEWAN TO CONDUCT THEIR BUSINESS INTERNATIONALLY, NATIONALLY AND LOCALLY FROM THEIR PLACE OF BUSINESS OR HOME. INTERNATIONAL MARKETS AND CONTACTS CAN BE ACCESSED EASILY AND LARGE QUANTITIES OF INFORMATION CAN BE EXCHANGED EFFICIENTLY.

PAGE FIVE

SECOND, THE NEW TECHNOLOGIES CREATE A VISTA OF NEW ECONOMIC OPPORTUNITIES. THE INFORMATION INDUSTRY THAT I ALLUDED TO EARLIER IS ONE THAT IS BEING ENCOURAGED BY THE GOVERNMENT OF SASKATCHEWAN. IT OFFERS OPPORTUNITIES IN BOTH SOFTWARE - THE KNOWLEDGE AND INFORMATION NECESSARY TO OPERATE OR USE THE NEW TECHNOLOGIES - AND HARDWARE, THE EQUIPMENT ITSELF. ADVANCEMENTS IN TECHNOLOGY, HOWEVER, FREQUENTLY ARE ACCOMPANIED BY SOCIAL CONCERNS. THE TECHNOLOGIES THAT ALLOW US TO PROCESS AND EXCHANGE INFORMATION OVER GREAT DISTANCES BRING WITH THEM CONCERNS FOR INDIVIDUALS AND OUR RIGHT TO CONTROL INFORMATION ABOUT OURSELVES.

YOU WILL APPRECIATE FROM EARLIER REMARKS ABOUT ADVANCES THAT HAVE BEEN MADE IN COMMUNICATIONS TECHNOLOGIES IN SASKATCHEWAN, THAT THE ISSUE OF PERSONAL INFORMATION BROUGHT ABOUT BY THE NEW TECHNOLOGIES IS A REALITY NOT A HYPOTHETICAL SITUATION. ACCORDINGLY, THE GOVERNMENT OF SASKATCHEWAN APPRECIATES THAT THIS IS AN IMPORTANT ISSUE AND ONE THAT REQUIRES EFFECTIVE ATTENTION. THIS APPRECIATION IS REINFORCED IN THE PROVINCE BECAUSE SASKTEL, THE PROVINCE'S TELCO, IS, AS I ALREADY MENTIONED, OWNED AND REGULATED BY THE PROVINCE. THIS MEANS THAT GOVERNMENT CAN ILL AFFORD TO HAVE ADVERTISERS OR INFORMATION VENDORS COMPROMISE THE PUBLIC.

PAGE SIX

IT WOULD SEEM, THEREFORE, THAT PROTECTION OF AN INDIVIDUAL'S RIGHTS WILL REQUIRE SOME FORM OF PUBLIC SECTOR INTERVENTION BY GOVERNMENTS.

THE CONCERN OVER THE ISSUE OF INFORMATION IS MORE WIDESPREAD THAN I HAVE SUGGESTED TO THIS POINT. THE EUROPEANS HAVE RECOGNIZED, ACKNOWLEDGED AND TAKEN MEASURES TO PROTECT ALL INDIVIDUALS' RIGHTS. THE COUNCIL OF EUROPE AND THE EEC HAVE CO-OPERATED TO DEVELOP A SET OF PRINCIPLES THAT ARE INTENDED TO GUIDE COUNTRIES IN THE PREPARATION OF LEGISLATION. A EUROPEAN CONVENTION RESPECTING PRIVACY HAS BEEN PASSED: PARTICIPATING COUNTRIES RATIFIED THE CONVENTION BY PASSING LEGISLATION.

GREAT BRITAIN IS ONE COUNTRY THAT IS IN THE PROCESS OF PASSING PRIVACY LEGISLATION. THIS LEGISLATION, WHICH WE WILL BE HEARING MORE ABOUT TOMORROW FROM THE HONOURABLE DAVID WADDINGTON, MINISTER OF STATE FOR THE HOME OFFICE:

- "... WILL ESTABLISH A DATA PROTECTION REGISTRAR, WHO WILL MAINTAIN A REGISTER OF PERSONAL DATA USERS AND COMPUTER BUREAUX AND POWERS TO ENSURE THAT DATA ARE USED IN ACCORDANCE WITH (CERTAIN) GENERAL PRINCIPLES ...;
- SETS UP AN APPEAL NETWORK FOR DATA USERS; AND

PAGE SEVEN

- GIVES DATA SUBJECTS CERTAIN LEGAL RIGHTS,
INCLUDING A RIGHT OF ACCESS TO THEIR PERSONAL DATA
AND IN CERTAIN CIRCUMSTANCES A RIGHT TO
COMPENSATION."

IT WOULD SEEM THAT THE ONUS FOR INTERVENTION BY GOVERNMENT IS STRONGLY EMPHASIZED WHEN ENVIRONMENTAL CONCERNS AND ISSUES LIKE PRIVACY BECOME TOO LARGE FOR THE INDIVIDUAL TO CONTROL HIMSELF. BUT IS THERE ANOTHER SIDE TO ISSUES OF THIS NATURE THAT NEEDS TO BE TAKEN INTO CONSIDERATION TO BALANCE PUBLIC SECTOR INTERVENTION? CONSIDER, FOR EXAMPLE, BENEFITS THAT ARE DERIVED FROM ADVANCES IN COMPUTING AND COMMUNICATIONS TECHNOLOGIES. CONSIDER ALSO, THE VENDORS OF THESE SERVICES. PUBLIC SECTOR INTERVENTION SHOULD NOT DEPRIVE SOCIETY OF BENEFITS NOR SMOTHER ENTERPRISE BUT INSTEAD SHOULD SEEK TO CREATE A CLIMATE AND FRAMEWORK TO FOSTER THE GOOD AND OBLITERATE THE EVIL. CAN LEGISLATION, SUCH AS THAT WHICH THE BRITISH GOVERNMENT IS INTRODUCING, ACHIEVE THIS?

PRIVATE SECTOR INTERESTS THAT ARE REPRESENTED BY ORGANIZATIONS LIKE THE CCTA OR FLEDGLING INFORMATION COMPANIES CAN BE ANTICIPATED TO ARGUE THAT LEGISLATION OR REGULATION WILL IMPAIR THEIR ABILITY TO PROVIDE THE TYPE OF SERVICE THE PUBLIC WISHES AT A REASONABLE PRICE. PUBLIC SECTOR INTERVENTION, PARTICULARLY LEGISLATION, FREQUENTLY IS PERCEIVED BY SUCH ORGANIZATIONS TO BE

PAGE EIGHT

BURDENSOME, EXPENSIVE AND A THREAT TO THE INFORMATION INDUSTRY. THIS, HOWEVER, NEED NOT BE THE CASE. LEGISLATION CAN ASSIST BOTH THE PUBLIC AND INFORMATION VENDORS. HOW CAN THIS BE, PARTICULARLY WITH AN INDUSTRY SUCH AS THE INFORMATION INDUSTRY THAT EMPLOYS SUCH NOVEL TECHNOLOGIES LIKE VIDEOTEX?

THE PROPOSED BRITISH LEGISLATION WHICH I CITED A FEW MOMENTS AGO AND WHICH WE WILL BE HEARING MORE ABOUT TOMORROW, HAS THE POTENTIAL TO PROTECT THE PUBLIC INTEREST AND TO HELP FOSTER AN INFORMATION INDUSTRY. THE REGISTRY CONCEPT AND ASSOCIATED REGULATIONS ON WHICH IT IS BASED, FACILITATES THE PUBLIC INTEREST BY ESTABLISHING THE RULES OF THE GAME AND THE SANCTIONS FOR NON-COMPLIANCE. INFORMATION COMPANIES OPERATING WITHIN THE FRAMEWORK OF THE LEGISLATION EFFECTIVELY WILL BE ACCOMMODATING PRIVACY CONCERNS AS DEFINED BY PUBLICLY RESPONSIBLE LEGISLATORS. THE PUBLIC, CONSEQUENTLY, WILL PERCEIVE THESE COMPANIES TO BE LAW ABIDING AND THUS WORTHY OF ITS TRUST. THIS PERCEPTION IS IMPORTANT TO INFORMATION VENDORS BECAUSE IT IS UNLIKELY THAT THE PUBLIC WOULD PATRONIZE THEM IF THEIR INTEGRITY WAS SUSPECT. THUS, LEGISLATION WOULD AFFORD A CERTAIN STATUS TO INFORMATION VENDORS, AND THIS STATUS WOULD HAVE VALUE IN BOTH MORAL AND COMMERCIAL TERMS.

PAGE NINE

COMMERCIAL INTERESTS COULD BE FURTHER SERVED BY LEGISLATION THAT EMPLOYS THE REGISTRY CONCEPT. THE AGENCY OF GOVERNMENT THAT REGISTERS AND POLICES INFORMATION VENDORS COULD MAKE THE LIST OF REGISTERED VENDORS AVAILABLE TO PATRONS. PUBLIC ATTENTION THUS WOULD BE DIRECTED TO THOSE COMPANIES THAT ARE KNOWN TO GOVERNMENT AND WHO ARE SUBJECT TO GOVERNMENT SANCTIONS IF THEY DO NOT CONFORM TO THE LEGISLATION THAT PROTECTS THE PUBLIC INTEREST. THIS TOO HAS COMMERCIAL VALUE AND CAN HELP TO FOSTER THE INDUSTRY BY ENSURING THAT COMPANIES OPERATING IN IT ARE HONOURABLE.

I BELIEVE THAT LEGISLATION WHICH EMBRACES THE REGISTRY CONCEPT IS WORTHY OF OUR CONSIDERATION AND ATTENTION. WORTHINESS IS AN IMPORTANT CONCEPT TO SASKATCHEWAN LEGISLATORS BECAUSE GOVERNMENT POLICY IN SASKATCHEWAN IS DIRECTED TOWARD REDUCING OR PRECLUDING REGULATIONS OR LEGISLATION THAT ARE NOT NECESSARY. I BELIEVE THAT THE CASE FOR LEGISLATION AS IT PERTAINS TO PERSONAL INFORMATION IS STRONG: I REITERATE THAT THE REGISTRY CONCEPT IN LEGISLATION SHOULD BE CONSIDERED. BUT, HOW CAN THIS COME ABOUT IN A COUNTRY WITH TWO SENIOR LEVELS OF GOVERNMENT AND SEVERAL JURISDICTIONS?

THE EUROPEANS AGAIN HAVE PROVIDED A MODEL THAT WE COULD FOLLOW IN PREPARING SUCH LEGISLATION. EARLIER IN MY REMARKS, I ALLUDED TO THE CONCEPT THEY HAVE EMPLOYED.

PAGE TEN

THIS INVOLVED THE RELEVANT COUNTRIES, OR JURISDICTIONS IN OUR CASE, DEVELOPING AND AGREEING TO A SET OF PRINCIPLES THAT WOULD ESTABLISH THE FRAMEWORK FOR LEGISLATION IN EACH JURISDICTION. COMMUNICATIONS BETWEEN THOSE INDIVIDUALS CHARGED WITH THE RESPONSIBILITY FOR CREATING LEGISLATION IN THEIR RESPECTIVE COUNTRIES HELPED TO ENSURE COMPATIBILITY AND ACCEPTABILITY AMONG COUNTRIES THAT AGREED TO THE SET OF PRINCIPLES.

THIS METHOD OF PROCEEDING COULD ACCOMMODATE THE TYPES OF CONCERNS THAT ARE EVIDENT IN THE RESPECTIVE LEVELS AND JURISDICTIONS OF GOVERNMENT IN CANADA; EACH JURISDICTION COULD HAVE ITS UNIQUE CIRCUMSTANCES ACCOMMODATED WITHOUT THREATENING THE GENERAL INTENT OF THE AGREED PRINCIPLES.

WE IN CANADA ARE FORTUNATE WITH RESPECT TO THIS ISSUE IN THAT A GREAT DEAL OF VALUABLE WORK, PRINCIPLES, LEGISLATION AND EXPERIENCE COULD BE DRAWN FROM THE EUROPEANS. FURTHERMORE, CANADA ITSELF HAS DONE A REASONABLE AMOUNT OF WORK THROUGH THE OECD. SHE HAS CONSULTED WITH THE PROVINCES ABOUT THE OECD GUIDELINES AND CURRENTLY IS DECIDING WHETHER OR NOT TO ADHERE TO THEM.

PAGE ELEVEN

CLEARLY, THE TIME OF DECISION WITH RESPECT TO THIS ISSUE IS AT HAND. WE HAVE THIS EXCELLENT FORUM GRACIOUSLY ORGANIZED BY THE GOVERNMENT OF ONTARIO. I BELIEVE THAT WE SHOULD AVAIL OURSELVES OF THIS OPPORTUNITY TO FOLLOW THE EUROPEAN MODELS, TO USE CANADA'S EXPERIENCE AND TO CREATE A LEGISLATIVE MOSAIC TO ENSURE THAT AN INDIVIDUAL'S RIGHT IS ENSURED AT LOCAL, NATIONAL AND INTERNATIONAL LEVELS. TO THIS END, I WOULD SUGGEST THAT THE LEVELS OF GOVERNMENT AND JURISDICTIONS THAT ARE REPRESENTED HERE ESTABLISH A COMMITTEE, THE MEMBERS OF WHICH WOULD BE CHARGED WITH TWO RESPONSIBILITIES: (1) CREATION OF A SET OF PRINCIPLES TO GUIDE THE DEVELOPMENT OF LEGISLATION IN THE RESPECTIVE JURISDICTIONS, FOR WHICH WE HAVE VALUABLE INFORMATION TO HELP THAT PROCESS ALONG, AND (2) ONCE THE PRINCIPLES HAVE BEEN AGREED TO, CO-ORDINATE THE DEVELOPMENT OF LEGISLATION IN THE RESPECTIVE JURISDICTIONS. I BELIEVE THAT LEGISLATION OF THE TYPE I HAVE DESCRIBED TODAY WILL PROTECT THE PUBLIC INTEREST, HELP TO FOSTER THE INFORMATION INDUSTRY AND ASSIST IN IMPROVING INTERNATIONAL RELATIONS THROUGH A MEDIUM THAT CAN ASSIST BOTH SOCIAL AND ECONOMIC WELL BEING.

THANK YOU.

CA 1
Z 4
- 032

DOCUMENT: 870-123/018

CONFÉRENCE INTERPROVINCIALE SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS:
MESURES POUR 1984 (COLLOQUE)

Notes en vue d'une allocution

prononcée par

Douglas Smith
Sous-ministre adjoint
Direction de la politique en matière de communications
Ministère de la Justice
Saskatchewan



Toronto (Ontario)
Les 23 et 24 mai 1984

Ce n'est pas de vie privée dont il est question à cette conférence. En effet, l'ère de l'électronique nous a amenés bien au delà des vieilles notions de vie privée. Les gens d'aujourd'hui doivent adopter de nouvelles attitudes sur cette question. Nous devons penser en fonction de nouvelles formes de protection des renseignements personnels.

Il est certain que des dossiers sont constitués à notre sujet: c'est le cas de quiconque a déjà demandé une hypothèque, une carte Visa, qui a visité un médecin, ouvert un compte de banque ou demandé l'une des quelque mille cartes de crédit qui sont disponibles. Pour jouir de l'avantage d'avoir accès au crédit, nous avons sciemment, ou involontairement, renoncé à notre vie privée.

Pour avoir l'avantage de retirer de l'argent de guichets automatiques lorsque les banques sont fermées, nous nous sommes mis à découvert. Certains parmi nous, les partisans de la liberté civile, voudraient que nous retournions à l'âge des ténèbres et nous faire croire qu'il est mauvais que des gens puissent obtenir des renseignements à notre sujet. Mais vous savez, le respect absolu de la vie privée est une notion relativement moderne. Celle-ci n'existait pas dans la Cité grecque et elle n'existe toujours pas dans les collectivités de 500 habitants. L'information au sujet des gens qui vivent dans des petites collectivités revêt en effet un caractère très public.

Cependant, ce qui inquiète les gens aujourd'hui, ce sont les volumes énormes d'information qui peuvent être emmagasinés à leur sujet, les formes que revêt cette information et le fait qu'elle puisse être mal utilisée.

("Data protection" - P. Flaherty.)

Voici en fait l'objet de cette conférence : non pas la vie privée, mais la mauvaise utilisation de l'information. C'est là qu'est la vraie question. Personnellement, cela ne me fait rien que les gens recueillent des renseignements à mon sujet, mais ce que je leur demande, c'est de ne pas utiliser ces renseignements pour me nuire. La question que nous devons résoudre est la suivante: "Y a-t-il des moyens de contrôler la mauvaise utilisation de ces renseignements? Comment pouvons-nous exiger des comptes des personnes qui recueillent des renseignements?"

D'ailleurs, cette question n'est pas nouvelle. Dans Othello, Shakespeare ne disait-il pas:

Qui me vole ma bourse, il vole un vil métal :
Cela ne compte point; la chose était à moi,
Elle est à lui et fut la chose de mille autres;
Mais, au contraire, qui m'ôte mon bon renom,
Il me soustrait un bien qui ne l'enrichit point
Et du coup m'appauvrit.

C'est certain qu'il n'y avait pas d'ordinateurs du temps de Shakespeare mais cela n'a pas empêché ce dernier d'être conscient du problème, tout comme nous le sommes en Saskatchewan. Mon ministre, l'honorable J. Gary Lane, est responsable de la société de téléphone de propriété publique, ainsi que de SaskComp, la plus grosse installation d'ordinateur dans notre province.

Mon ministre, mon gouvernement finalement, tient sincèrement à faire en sorte que le système de la société de téléphone ne soit pas mal utilisé par ceux qui veulent transmettre de l'information par son entremise. Par ailleurs, cette préoccupation est modérée par le fait que nous savons qu'un recours trop strict ou trop sévère à des lois ou à des conditions imposées aux usagers peut étouffer l'esprit d'initiative nécessaire à la mise sur pied de la myriade de nouveaux services de télécommunications qui sont déjà en place ou qui se profilent déjà à l'horizon.

Comme plusieurs d'entre vous le savez déjà, la Saskatchewan possède le système de fibre optique le plus long au monde. Sa capacité est extraordinaire et il présente d'énormes possibilités pour les données à double interaction. Au cours des toutes dernières années, nous avons également acquis une expérience incalculable grâce à des réseaux d'information tels que le "Pathfinder Trial" et le service "Agritex" maintenant en place.

L'expérience acquise grâce au projet Pathfinder a aidé les vendeurs d'information et Sasktel à élaborer un arrangement plus perfectionné en matière de vidéotex. Cela permettra aux abonnés qui disposent du matériel approprié d'avoir accès à des renseignements à partir de l'une de nombreuses bases de données potentielles situées dans des endroits éloignés et indépendants. Cela est rendu possible parce que Sasktel est maintenant propriétaire et exploitant d'un ordinateur tête de ligne qui facilite le raccordement des usagers à la base de données dont ils ont besoin et favorise le processus de facturation nécessaire. Le service de transit qu'offre Sasktel est le premier service commercial de ce genre en Amérique du Nord. Le service est appelé Agritex et les bases de données disponibles par son entremise peuvent être utilisées grâce à l'une ou l'autre de deux formules.

Quelles sont les incidences de ces techniques et services pour le public? La première conséquence importante tient à ce que nos services de communication permettent aux gens d'affaires et aux résidants de la Saskatchewan de faire des affaires sur la scène internationale, nationale ou locale à partir de leur bureau ou de leur résidence. Les marchés et les contacts internationaux peuvent être rejoints facilement et il est possible d'échanger d'importants volumes d'information de façon rentable.

En deuxième lieu, les nouvelles techniques créent une vue d'ensemble des nouvelles perspectives économiques. L'industrie de l'information dont j'ai déjà parlé est parmi celles qui sont encouragées par le gouvernement de la Saskatchewan. Elle offre des possibilités tant en matière de logiciel, c'est-à-dire les connaissances et les renseignements nécessaires pour exploiter ou utiliser les nouvelles techniques, que de matériel, c'est-à-dire l'équipement proprement dit. Cependant, les percées technologiques s'accompagnent souvent de préoccupations sociales. Les techniques qui nous permettent de traiter et d'échanger des renseignements à grande distance suscitent des craintes pour les particuliers et leur droit de contrôler les renseignements qui les concernent.

À la lumière des observations précédentes au sujet des progrès qui ont été réalisés en matière de techniques de communication en Saskatchewan, vous reconnaîtrez que la question soulevée par les nouvelles techniques en matière de renseignements personnels est bel et bien une réalité et non pas une situation hypothétique. Par conséquent, le gouvernement de la Saskatchewan reconnaît l'importance de cette question et estime qu'elle doit recevoir toute l'attention nécessaire. Cette position est renforcée dans la province par le fait que Sasktel, la société de téléphone de la province, est, comme je l'ai déjà mentionné, propriété de la province, qui la réglemente également. Cela signifie que le gouvernement ne peut pas se permettre

de laisser les annonceurs ou les vendeurs d'information compromettre le public. C'est donc dire qu'il semble que la protection des droits d'un particulier nécessite une certaine forme d'intervention des gouvernements dans le secteur public.

Les craintes suscitées par la question de l'information sont plus répandues que ne l'a laissé supposer mon intervention jusqu'ici. Les Européens ont reconnu et officialisé tous les droits des particuliers et pris des mesures visant à les protéger. Le Conseil de l'Europe et la CEE ont collaboré afin d'élaborer un ensemble de principes visant à guider les pays lors de la préparation des lois. Une convention européenne en matière de protection de la vie privée a été adoptée: les pays participants ont ratifié la convention par l'adoption de lois pertinentes.

La Grande-Bretagne est en voie d'adopter une loi en la matière. Cette loi, dont l'honorable David Waddington, ministre d'État au ministère de l'Intérieur, nous reparlera plus longuement demain,

(traduction non officielle)

- "... établit le poste de registraire de la protection des données, qui maintiendra un répertoire des usagers de données personnelles et des bureaux d'informatique et

sera doté de pouvoirs lui permettant de veiller à ce que les données soient utilisées conformément à (certains) principes généraux ...;

- établit un réseau d'appel pour les usagers des données;
et
- accorde aux personnes qui sont l'objet des données certains droits juridiques, notamment le droit d'accès aux données qui les concernent et, en certaines circonstances, le droit à une indemnisation."

De toute évidence, le fait qu'il incombe au gouvernement d'intervenir est d'autant plus accentué lorsque les préoccupations et les questions touchant l'environnement, comme la protection des renseignements personnels, prennent trop d'ampleur pour que le particulier puisse les contrôler lui-même. Mais pour les questions de cette nature, y-a-t-il un autre élément dont il convient de tenir compte en contrepartie de l'intervention du secteur public? Pensons par exemple aux avantages que comportent les progrès qui ont été réalisés dans les techniques de communication et d'informatique. Pensons également aux vendeurs de ces services. L'intervention du secteur public ne devrait pas priver la société d'avantages certains ni étouffer l'entreprise mais au contraire tenter de créer un climat et un cadre qui favorisent

les bonnes choses et suppriment les mauvaises. Une loi comme celle que le gouvernement britannique propose peut-elle y parvenir?

Le secteur privé dont les intérêts sont représentés par les organismes comme la CCTA ou de toutes nouvelles sociétés d'information peuvent soutenir, il faut s'y attendre, que des lois ou des règlements nuiront à leur capacité de fournir le type de service que veut le public à un prix raisonnable. Les organisations de ce genre perçoivent souvent l'intervention du secteur public, et plus particulièrement les mesures législatives, comme étant toujours lourdes, coûteuses et menaçantes pour l'industrie de l'information. Or, il ne doit pas nécessairement en être ainsi. Une loi peut aider tant le public que les vendeurs d'information. Comment y arriver, particulièrement dans le cas d'une industrie comme celle de l'information qui utilise des techniques de pointe comme le vidéotex?

Le projet de loi britannique dont j'ai parlé il y a quelques instants, et au sujet duquel nous aurons plus de renseignements demain, offre la possibilité de protéger l'intérêt public et d'aider à la croissance de l'industrie de l'information. Le concept de registre et les règlements connexes sur lesquels il se fonde favorisent l'intérêt public en fixant les règles du jeu et

les sanctions prévues dans le cas d'infraction. Les sociétés d'information qui fonctionneront dans le cadre de la loi tiendront en fait compte des préoccupations en matière de protection des renseignements personnels telles qu'elles sont définies par des législateurs responsables à l'égard de la population. Par conséquent, le public percevra ces sociétés comme étant respectueuses des lois et, partant, dignes de sa confiance. Cette perception est importante pour les vendeurs d'information car il est peu probable que les gens voudront être leurs clients si leur intégrité est mise en doute. C'est donc dire que la loi accorderait un certain statut aux vendeurs d'information et que ce statut aura de la valeur sur les plans tant moral que commercial.

Les intérêts commerciaux pourraient en outre être mieux défendus par une loi qui s'appuie sur le concept de l'enregistrement. L'organisme du gouvernement qui enregistre et régit les vendeurs d'information pourrait mettre à la disposition des clients la liste des vendeurs enregistrés. La population saurait ainsi quelles sont les sociétés qui sont connues du gouvernement et assujetties à des sanctions de sa part si elles ne se conforment pas aux lois qui protègent l'intérêt public. Cela aussi a une valeur commerciale et peut aider l'industrie à s'épanouir en garantissant le caractère honorable des sociétés qui oeuvrent sur le marché.

Je crois qu'une loi qui intègre le principe de l'enregistrement est digne de notre attention. Le caractère valable des mesures importe beaucoup aux législateurs de la Saskatchewan car la politique du gouvernement en Saskatchewan vise à réduire ou à éviter des règlements ou des lois inutiles. Je crois que le recours à une loi dans le domaine des renseignements personnels se justifie amplement : je persiste à dire qu'il y a lieu d'envisager le concept d'un enregistrement par voie législative. Cependant, comment y parvenir dans un pays qui compte deux principaux ordres de gouvernement et plusieurs administrations?

Une fois de plus, les Européens ont conçu un modèle auquel nous pouvons nous reporter dans la préparation de pareilles lois. J'ai déjà fait allusion au concept qu'ils ont utilisé. Dans ce processus, les pays visés, qui seraient des administrations dans notre cas, ont élaboré et adopté un ensemble de principes devant régir le cadre législatif dans chaque administration. Les communications établies entre les personnes chargées de créer les lois dans leurs pays respectifs ont aidé à assurer la compatibilité et le caractère acceptable des principes dans les pays qui ont convenu de les adopter.

Cette façon de procéder permettrait de tenir compte des diverses préoccupations qui caractérisent les différents ordres de gouvernement et administrations au Canada; il serait possible de tenir compte de la situation particulière à chaque administration sans nuire pour autant à l'intention générale des principes convenus.

Au Canada, nous sommes chanceux dans ce domaine en ce sens que nous pouvons profiter de la somme considérable de travaux, principes, lois et expériences valables des Européens. De plus, le Canada a lui-même fourni un travail considérable par l'intermédiaire de l'OCDE. Il a consulté les provinces au sujet des directives de l'OCDE et est actuellement en voie de décider s'il y adhèrera ou non.

De toute évidence, l'heure de la décision approche. Le gouvernement de l'Ontario a gracieusement organisé à notre intention cet excellent cadre de discussions. Je crois que nous devrions profiter de l'occasion pour suivre les modèles européens, nous prévaloir de l'expérience canadienne et créer une mosaïque législative grâce à laquelle le droit des particuliers sera garanti à l'échelle locale, nationale et internationale. À cette fin, je propose que les ordres de gouvernement et les administrations ici représentés mettent sur pied un comité dont les membres auraient deux responsabilités : (1) la création d'un ensemble de principes guidant l'élaboration de lois dans les administrations respectives, processus qui sera facilité par les renseignements valables dont nous disposons déjà, et (2) une fois les principes convenus, la coordination de l'élaboration des lois dans les administrations respectives. Je crois qu'une loi semblable à celle que j'ai décrite aujourd'hui protégera l'intérêt public, favorisera l'épanouissement de l'industrie de

l'information et aidera à l'amélioration des relations internationales grâce à un outil susceptible d'être favorable au bien-être socio-économique de la population.

Merci.

INTERPROVINCIAL CONFERENCE ON PRIVACY:
INITIATIVES FOR 1984 (SYMPOSIUM)

CONFÉRENCE INTERPROVINCIALE SUR LA PROTECTION
DES RENSEIGNEMENTS PERSONNELS : MESURES POUR 1984 (COLLOQUE)

Toronto

May 23-24, 1984

Les 23 et 24 mai 1984

LIST OF PUBLIC DOCUMENTS

LISTE DES DOCUMENTS PUBLICS

DOCUMENT NO. N° DU DOCUMENT	SOURCE ORIGINE	TITLE TITRE
870-123/001	Conference Conférence	Program Programme
870-123/003	Secretariat Secrétariat	✓ Final List of Delegates Liste définitive des délégués
870-123/004	Ontario	Discussion Paper on Privacy: Initiatives for 1984 Document de travail sur la vie privé : Projets pour 1984
870-123/005	Hugh V. O'Neill American Soc. of Access Professionals	✓ Abstract: Fair Information Practice and Computers ✓ Résumé : Les pratiques loyales en matière d'information et le secteur de l'information

DOCUMENT NO. N° DU DOCUMENT	SOURCE ORIGINE	TITLE TITRE
870-123/006	Rodney H. Cooper, University of New Brunswick and Wayne Patterson Moncton Univ.	✓ Why Computer Scientists and the Computing Profession Must Work to Shape Impending Legislation (From: Proceedings, Canadian Information Processing Society - Session '84)
	Rodney H. Cooper, Université de Nouveau-Brunswick et Wayne Patterson, Université de Moncton	✓ Raisons pour lesquelles les informaticiens et le secteur de l'informatique doivent chercher à influencer sur les projets de loi futurs (Extraits des comptes rendus des séances de 1984 de l'Association canadienne de l'informatique)
870-123/007	Thomas L. McPhail, Ph.D. University of Calgary	✓ Transborder Data Flow (TBDF) & The Continental Communication Pact (CCP): The Rationale for a Communication Pact
	Thomas L. McPhail, Ph.D., Université de Calgary	✓ La transmigration des données (TMO) et le Pacte continental sur les communications (PCC): la justification d'un Pacte sur les communications
870-123/008	Ralph Hancox Reader's Digest	✓ Notes for Conference ✓ Notes en vue d'une allocution
870-123/009	John D. McCamus York University	✓ The Delicate Balance: Reconciling Privacy Protection with the Freedom of Information Principle
	John D. McCamus Université York	✓ Un équilibre fragile : comment concilier la protection des renseignements personnels avec le principe de la liberté d'accès à l'information
870-123/010	Ontario	✓ Notes for an Address by: The Honourable Norman Sterling, Q.C., Provincial Secretary for Resources Development ✓ Notes préparées pour une allocution de l'honorable Norman Sterling, C.R., Secrétaire provincial au Développement des ressources
870-123/011	T. Murray Rankin University of Victoria	✓ Access to Information & Barriers for Privacy: The Search for Balance
	T. Murray Rankin Université de Victoria	✓ L'accès à l'information et les limites de la vie privée: A la recherche d'un équilibre

DOCUMENT NO. N° DU DOCUMENT	SOURCE ORIGINE	TITLE TITRE
870-123/012	James L. Kirschbaum Fireman's Fund Insurance Co.	Privacy Issues: The Property & Casualty Insurance Industry ✓ La protection des renseignements personnels: l'industrie de l'assurance risques divers
870-123/013	Ross W. McFarlane, Q.C., General Motors of Canada Ross W. McFarlane, General Motors of Canada	✓ Privacy: The Problems Defined ✓ La protection des renseignements personnels: Définition des problèmes
870-123/014	Dr. W. Ghent Canadian Medical Assoc. le docteur W. Ghent L'Association médicale canadienne	✓ Presentation By: Dr. W. Ghent, Chairman of the Council on Health Care for the Canadian Medical Association ✓ Allocution par le docteur W. Ghent, Président du Conseil des soins de santé de l'Association médicale canadienne
870-123/015	Eric Wimberley Cdn. Cable T.V. Assoc. Eric Wimberley Association canadienne de télévision par câble	✓ Presentation By: Eric Wimberley, Vice-President, Association Affairs, Canadian Cable Television Association ✓ Exposé de Eric Wimberley, Vice-président, Affaires de l'Association, Association canadienne de télévision par câble
870-123/016	James C. Grant Royal Bank of Canada James. C. Grant La Banque Royale de Canada	✓ Remarks to a Panel Discussion on "Transborder Data Flow: The Trends, The Issues" ✓ Remarques adressées à un groupe de travail sur "La transmigration des données : tendances et problèmes"

DOCUMENT NO. N° DU DOCUMENT	SOURCE ORIGINE	TITLE TITRE
870-123/017	Caroline Pestieau Quebec Access to Info. Comm.	Notes for a Presentation By: Caroline Pestieau, Commissioner, Quebec Access to Information Commission
	Caroline Pestieau Commission d'accès à l'information du Québec	Notes en vue d'une allocution prononcée à la Commission d'accès à l'information du Québec
870-123/018	Douglas Smith Saskatchewan	Notes for a Presentation by: Douglas Smith, Assistant Deputy Minister, Communications Policy Branch, Department
		Notes en vue d'une allocution prononcée par Douglas Smith, Sous-ministre adjoint à la direction de la politique en matière de communications, Ministère de la Justice, Saskatchewan
870-123/019 (a)	Quebec	Bill 65 - An Act respecting Access to documents held by public bodies and the Protection of personal information - Assented to 23 June 1982
	Québec	Projet de loi n° 65 - Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels - Sanctionné le 23 juin 1982
870-123/021	Secretariat Secrétariat	List of Public Documents Liste des documents publics
		(a) This document is available by writing to: Ce document est disponible en écrivant à : Librairie de l'Editeur officiel du Québec 662 St-Joseph Blvd., Hull, Québec J8Y 4A8

DOCUMENT: 870-123/021

+ 870-135 s

INTERPROVINCIAL CONFERENCE ON PRIVACY:
INITIATIVES FOR 1984 (SYMPOSIUM)CONFÉRENCE INTERPROVINCIALE SUR LA PROTECTION
DES RENSEIGNEMENTS PERSONNELS : MESURES POUR 1984 (COLLOQUE)

Toronto

May 23-24, 1984

Les 23 et 24 mai 1984

LIST OF PUBLIC DOCUMENTS

LISTE DES DOCUMENTS PUBLICS

DOCUMENT NO. N° DU DOCUMENT	SOURCE ORIGINE	TITLE TITRE
870-123/001	✓ Conference ✓ Conférence	Program Programme
870-123/003	Secretariat Secrétariat	✓ Final List of Delegates ✓ Liste définitive des délégués
870-123/004	Ontario	✓ Discussion Paper on Privacy: Initiatives for 1984 ✓ Document de travail sur la vie privé : Projets pour 1984
870-123/005	Hugh V. O'Neill American Soc. of Access Professionals	✓ Abstract: Fair Information Practice and Computers ✓ Résumé : Les pratiques loyales en matière d'information et le secteur de l'information

DOCUMENT NO. N° DU DOCUMENT	SOURCE ORIGINE	TITLE TITRE
870-123/006	Rodney H. Cooper, University of New Brunswick and Wayne Patterson Moncton Univ. Rodney H. Cooper, Université de Nouveau-Brunswick et Wayne Patterson, Université de Moncton	✓ Why Computer Scientists and the Computing Profession Must Work to Shape Impending Legislation (From: Proceedings, Canadian Information Processing Society - Session '84) ✓ Raisons pour lesquelles les informaticiens et le secteur de l'informatique doivent chercher à influencer sur les projets de loi futurs (Extraits des comptes rendus des séances de 1984 de l'Association canadienne de l'informatique)
870-123/007	Thomas L. McPhail, Ph.D. University of Calgary Thomas L. McPhail, Ph.D., Université de Calgary	✓ Transborder Data Flow (TBDF) & The Continental Communication Pact (CCP): The Rationale for a Communication Pact ✓ La transmigration des données (TMO) et le Pacte continental sur les communications (PCC): la justification d'un Pacte sur les communications
870-123/008	Ralph Hancox Reader's Digest	✓ Notes for Conference ✓ Notes en vue d'une allocution
870-123/009	John D. McCamus York University John D. McCamus Université York	✓ The Delicate Balance: Reconciling Privacy Protection with the Freedom of Information Principle ✓ Un équilibre fragile : comment concilier la protection des renseignements personnels avec le principe de la liberté d'accès à l'information
870-123/010	Ontario	✓ Notes for an Address by: The Honourable Norman Sterling, Q.C., Provincial Secretary for Resources Development ✓ Notes préparées pour une allocution de l'honorable Norman Sterling, C.R., Secrétaire provincial au Développement des ressources
870-123/011	T. Murray Rankin University of Victoria	✓ Access to Information & Barriers for Privacy: The Search for Balance

DOCUMENT NO. N° DU DOCUMENT	SOURCE ORIGINE	TITLE TITRE
870-123/012	James L. Kirschbaum Fireman's Fund Insurance Co.	✓ Privacy Issues: The Property & Casualty Insurance Industry ✓ La protection des renseignements personnels: l'industrie de l'assurance risques divers
870-123/013	Ross W. McFarlane, Q.C., General Motors of Canada Ross W. McFarlane, General Motors of Canada	✓ Privacy: The Problems Defined ✓ La protection des renseignements personnels: Définition des problèmes
870-123/014	Dr. W. Ghent Canadian Medical Assoc. le docteur W. Ghent L'Association médicale canadienne	✓ Presentation By: Dr. W. Ghent, Chairman of the Council on Health Care for the Canadian Medical Association ✓ Allocution par le docteur W. Ghent, Président du Conseil des soins de santé de l'Association médicale canadienne
870-123/015	Eric Wimberley Cdn. Cable T.V. Assoc. Eric Wimberley Association canadienne de télévision par câble	✓ Presentation By: Eric Wimberley, Vice-President, Association Affairs, Canadian Cable Television Association ✓ Exposé de Eric Wimberley, Vice-président, Affaires de l'Association, Association canadienne de télévision par câble
870-123/016	James C. Grant Royal Bank of Canada James. C. Grant La Banque Royale de Canada	✓ Remarks to a Panel Discussion on "Transborder Data Flow: The Trends, The Issues" ✓ Remarques adressées à un groupe de travail sur "La transmigration des données : tendances et problèmes"

DOCUMENT NO. N° DU DOCUMENT	SOURCE ORIGINE	TITLE TITRE
870-123/017	<p>Caroline Pestieau Quebec Access to Info. Comm.</p> <p>Caroline Pestieau Commission d'accès à l'information du Québec</p>	<p>Notes for a Presentation By: Caroline Pestieau, Commissioner, Quebec Access to Information Commission</p> <p>Notes en vue d'une allocution prononcée à la Commission d'accès à l'information du Québec</p>
870-123/018	Douglas Smith Saskatchewan	<p>Notes for a Presentation by: Douglas Smith, Assistant Deputy Minister, Communications Policy Branch, Department</p> <p>Notes en vue d'une allocution prononcée par Douglas Smith, Sous-ministre adjoint à la direction de la politique en matière de communications, Ministère de la Justice, Saskatchewan</p>
870-123/019	<p>Quebec</p> <p>Québec</p>	<p>Bill 65 - An Act respecting Access to documents held by public bodies and the Protection of personal information - Assented to 23 June 1982</p> <p>Projet de loi n° 65 - Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels - Sanctionné le 23 juin 1982</p>
870-123/021	<p>Secretariat</p> <p>Secrétariat</p>	<p>List of Public Documents</p> <p>Liste des documents publics</p>
870-135/005	Alberta	<p>Sub-Committee Report "National Coaching Certification Program"</p> <p>(French available)</p>
870-135/006	Alberta	<p>Procedural Guidelines 1986</p> <p>(French available)</p>

02.03.87

DOCUMENT: 870-165/028

PROVINCIAL-TERRITORIAL MEETING OF DEPUTY MINISTERS
RESPONSIBLE FOR SPORT AND RECREATION

RÉUNION PROVINCIALE-TERRITORIALE DES SOUS-MINISTRES
RESPONSABLES DU SPORT ET DES LOISIRS

CALGARY, Alberta
September 10, 1986



CALGARY (Alberta)
Le 10 septembre 1986

LIST OF PUBLIC DOCUMENTS

LISTE DES DOCUMENTS PUBLICS

MENT NO. DOCUMENT	SOURCE ORIGINE	TITLE TITRE
65/007	Alberta	Recreation Strategies for the Promotion of Health
	Alberta	Stratégies de promotion de la santé par les loisirs
65/017	Federal	Sport Marketing Council
	Fédéral	Conseil de marketing du sport
65/023	Federal	Women in Sport Policy
	Fédéral	Politique concernant les femmes et le sport

PROVINCIAL-TERRITORIAL MEETING OF DEPUTY MINISTERS
RESPONSIBLE FOR CULTURE AND HISTORICAL RESOURCES

RÉUNION PROVINCIALE-TERRITORIALE DES SOUS-MINISTRES
RESPONSABLES DE LA CULTURE ET DES RICHESSES HISTORIQUES

WINNIPEG, Manitoba
December 13, 1988

WINNIPEG (Manitoba)
Le 13 décembre 1988

LIST OF PUBLIC DOCUMENTS

LISTE DES DOCUMENTS PUBLICS

DOCUMENT NO. U DOCUMENT	SOURCE ORIGINE	TITLE TITRE
193/012	Manitoba	Historical Significance of the Forks Importance historique des "Forks"
193/017	Secretariat Secrétariat	List of Public Documents Liste des documents publics

21.01.93

DOCUMENT: 870-225/006

PROVINCIAL-TERRITORIAL MEETING OF DEPUTY MINISTERS
RESPONSIBLE FOR LABOUR MARKET MATTERS

RÉUNION PROVINCIALE-TERRITORIALE DES SOUS-MINISTRES
RESPONSABLES DES QUESTIONS RELATIVES AU MARCHÉ DU TRAVAIL

TORONTO, Ontario
May 27, 1992

TORONTO (Ontario)
Le 27 mai 1992

LIST OF PUBLIC DOCUMENTS

LISTE DES DOCUMENTS PUBLICS

DOCUMENT NO. NUMÉRO DU DOCUMENT	SOURCE ORIGINE	TITLE TITRE
✓ 870-225/004	Ontario	Red Seal/The Interprovincial Computerized Examination Management System
✓ 870-225/006	Secretariat Secrétariat	Sceau Rouge/Système interprovincial de gestion informatisés des examens List of Public Documents Liste des documents publics





21.01.93

Government
Publications

DOCUMENT: 870-226/048

MEETING OF THE INTERPROVINCIAL SPORT AND RECREATION COUNCIL

RÉUNION DU CONSEIL INTERPROVINCIAL DU SPORT ET DES LOISIRS

TORONTO, Ontario
June 2 and 4, 1992TORONTO (Ontario)
Les 2 et 4 juin 1992

LIST OF PUBLIC DOCUMENTS

LISTE DES DOCUMENTS PUBLICS

DOCUMENT NO. NUMÉRO DU DOCUMENT	SOURCE ORIGINE	TITLE TITRE
870-226/032	British Columbia	Sport Funding Guidelines and Procedures 1992/93 A copy may be obtained from: Ministry of Municipal Affairs, Recreation and Housing - Province of British Columbia
870-226/033	British Columbia	Sport Macroscopic : A Planning Guide for Provincial Sport Organizations 1992/93 A copy may be obtained from: Ministry of Municipal Affairs, Recreation and Housing - Province of British Columbia
870-226/034	British Columbia	Responding to the Challenge: A Strategic Leadership Role for the "Recreation and Community Services Branch" A copy may be obtained from: Ministry of Municipal Affairs, Recreation and Housing - Province of British Columbia
870-226/035	British Columbia	Sport and Recreation Grants for Fiscal Year: 1990/91 A copy may be obtained from: Ministry of Municipal Affairs, Recreation and Housing - Province of British Columbia
870-226/040	FPTFC	National Fitness/Active Living Organizational Summary
870-226/048	Secretariat Secrétariat	List of Public Documents Liste des documents publics

